CENTRAL BANK OF CYPRUS

DIRECTIVE TO CREDIT INSTITUTIONS ON GOVERNANCE AND MANAGEMENT ARRANGEMENTS IN CREDIT INSTITUTIONS

N.B. This translation of the Directive is unofficial. It has been prepared by the Central Bank of Cyprus for information purposes. The Central Bank of Cyprus shall not be responsible for its content. The official text is in the Greek language

JULY 2014

TABLE OF CONTENTS

PART XIV - MISCELLANEOUS

BUSINESS OF CREDIT INSTITUTIONS LAWS OF 1997 TO (No. 4) of 2013

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

The Central Bank of Cyprus, exercising the powers conferred to it by sections 19 and 41(1)-(2) of the Credit Institutions Laws of 1997 to (No. 4) of 2013, issues this Directive.

PART I
TITLE, SCOPE AND LEVEL OF APPLICATION AND DEFINITIONS

Short title.

1. This Directive shall be cited as the Governance and Management Arrangements Directive of 2014.

Purpose of the Directive.

2. The purpose of this Directive is to:

(a) set requirements on the governance structures of credit institutions;

(b) set requirements on the roles and responsibilities of the management body and senior management;

(c) set requirements on the development, implementation, and effective oversight of compliance, risk management and internal control frameworks.

Level of application.

3. (1) This Directive shall apply to authorised credit institutions incorporated in the Republic on an individual basis, unless Central Bank makes use of the derogation provided for in Article 7 of Regulation (EU) No 575/2013.

(2) Parent undertakings and subsidiaries subject to this Directive under subparagraph (1) shall –

(a) meet the obligations under this Directive on a consolidated or sub-consolidated basis to ensure that their arrangements, processes and mechanisms required by this Directive are consistent and well-integrated 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 under subparagraph (1) to ensure that these arrangements, processes and mechanisms are consistent and well-integrated and those subsidiaries are able to produce any data and information relevant to the purpose of supervision;

(3) Obligations resulting from this Directive concerning subsidiary undertakings, not themselves subject to this Directive, shall not apply if the EU parent institution or institutions controlled by an EU parent financial holding company or EU parent mixed financial holding company, can demonstrate to the Central Bank that the application of this

Directive is unlawful under the laws of the third country where the subsidiary is established.

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

(5) The Central Bank may request the compliance of credit institutions incorporated in a member state which operate through a branch in the Republic, with provisions of this Directive as far as their Cyprus based branches are concerned, if their Cyprus based branches are considered significant in accordance with Section 27E of the Law.

(6) The Central Bank may request the compliance of credit institutions incorporated in a third country which operate through a branch in the Republic, with provisions of this Directive as far as their Cyprus based branches are concerned, after taking into account the significance of their operations in the Republic to the stability of the banking system, the group to which they belong and the extent of the institution's management and control exercised in or from within the Republic.

Definitions.

4. For the purposes of this Directive, the interpretations referred to in the Law and in the Regulation (EU) No 575/2013 shall apply, unless the context otherwise requires; additionally, the following interpretations are applicable, unless the context otherwise requires:

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

"code of business conduct and corporate values" means the set of principles, values, standards, or rules of behaviour that guide the decisions, procedures and systems of an institution in accordance with Part VII;

"committee" means a subgroup of the management body mandated to carry out specified functions or projects assigned;

"company secretary" means the chief administrative officer of a company incorporated under the Companies Law appointed under Section 171 of the Companies, responsible along with the directors for certain tasks under the Companies Law and any other person that may carry out the duties of a company secretary in accordance with this Directive;

"compliance culture" means the set of the combined set of individual and corporate values, attitudes, competencies and behaviour that determine an institution's commitment to and

style of compliance with internal and external rules and regulations;

“executive member of the management body” has the meaning attributed to this term in paragraph 2 the Fitness and Probity Directive of 2014;

“external auditor” means a statutory auditor or audit firm in accordance with the provisions of the Auditors and Statutory Audits of Annual and Consolidated Accounts Law of 2009 as subsequently amended or replaced and includes the approved auditor of the institution;

“independent member of the management body” has the meaning attributed to this term in paragraph 2 of the Fitness and Probity Directive of 2014;

“institution” means authorised credit institution and significant branch of EU credit institution that are subject to the provisions of this Directive;

“internal control functions” are consisted of a risk management function, a compliance function, an information security function and an internal audit function as provided by paragraph 76 of this Directive;

“Law” means the Business of Credit Institutions Laws of 1997 to (No. 4) of 2013;

“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 model, due to errors in the development, implementation or use of such models;

“outsourcing” means the use of a third party to perform services or activities that would normally be undertaken by the institution, now or in the future and does not include the purchase of products or services;

“purchase of products or services” means inter alia the supply of -

(i) standardized products, such as market information or information on current prices and purchase of office inventory and other goods and consumables; and
(ii) counseling and other services that are not part of the business and investment activities of the institution, including legal advice;

“risk appetite” means the aggregate level and types of risk an institution is willing to assume within its risk capacity to achieve its business objectives and strategies;

“risk capacity” means the maximum level of risk the institution can assume before breaching constraints determined by regulatory capital and liquidity needs and its obligations to depositors, other customers, and shareholders;

“risk culture” means the set of the combined set of individual and corporate values, attitudes, competencies and behaviour that determine an institution’s commitment to and

style of risk management;

“risk profile” means a point in time assessment of an institution’s risk exposures after taking into account risk mitigation aggregated within and across each relevant risk category based on forward looking assumptions;

PART II
GENERAL REQUIREMENTS

General requirements.

5. (1) The management body has the primary responsibility for internal governance at all times; It must define, oversee and shall be accountable for the implementation of governance arrangements that ensure effective and prudent management of the institution, including the segregation of duties and the prevention of conflicts of interest.

(2) The arrangements referred to in subparagraph (1) shall comply with the following principles:

(a) the management body must have the overall responsibility for the institution and approve and oversee the implementation of the institution's strategic objectives, risk strategy and internal governance;

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

(c) the management body must oversee the process of disclosure and communications;

(d) the management body must be responsible for providing effective oversight of senior management;

(3) The management body must monitor and periodically assess the effectiveness of the institution's governance arrangements and takes appropriate steps to address any deficiencies.

(4) Where the institution is the parent undertaking of a group of companies, its management body shall have the overall responsibility for adequate internal governance across the group; in order to fulfil its internal governance responsibilities, the management body of the institution should:

(a) establish a governance structure which contributes to the effective oversight of its subsidiaries and takes into account the nature, scale and complexity of the different risks to which the group and its subsidiaries are exposed;

(b) approve an internal governance policy at the group level, which includes the commitment to meet all applicable governance requirements;

(c) ensure that enough resources are available for each subsidiary to meet both group standards and local governance standards;

(d) have appropriate means to monitor that each subsidiary complies with all applicable internal governance requirements; and

(e) ensure that reporting lines in a group should be clear and transparent, especially where business lines do not match the legal structure of the group.

(5) In group structures where an institution is a subsidiary, its management body should apply the governance arrangements, processes and mechanisms developed at group level unless legal and supervisory requirements in the Republic or proportionality considerations determine otherwise; in this regard, the management body must evaluate any group level governance decisions or practices to ensure they -

(a) are not in breach of the provisions of the Regulation (EU) No 575/2013, the Law and Directives issued under the Law and, where applicable, other legislation or standards;

(b) are not detrimental to -

(i) the sound and prudent management of the institution;

(ii) the financial health of the institution;

(iii) the legal interests of the institution's stakeholders.

PART III
MANAGEMENT BODY

Section 1 –Composition, organisation and functioning of the management body and access to information and resources

Size and composition of the management body.

6. The size and composition of the management body must be set by taking into account the size and complexity of the institution and the nature and scope of its activities ensuring that –

(a) the management body consists of not less than seven (7) members and not more than thirteen (13) members;

(b) at least fifty percent (50%) of the members of the management body rounded down plus one (1) member are independent in accordance with Section 19B of the Law;

(c) the executive members must be at least two (2) and not more than twenty five percent (25%) of the members of the management body rounded down, one of which must be the chief executive;

(d) the management body is sufficiently diverse as regards age, gender and educational and professional background to reflect an adequately broad range of experiences and facilitate a variety of independent opinions and critical challenge;

(e) the management body possesses adequate collective knowledge, skills and experience to be able to understand the institution's activities, including the main risks;

it is provided that, members may not appoint alternate members to represent them in their absence.

Organisation and functioning of the management body.

7. Institutions must have in place appropriate internal governance policies, practices and procedures for the organisation and functioning of the management body in accordance with the Law and this Directive that ensure the following:

(1) with regards to the organisational structure of the management body:

(a) an independent member of the management body holds the position of the chairperson of the management body in accordance with the provisions of Section 19B of the Law;

(b) a non-executive member of the management body holds the position of the vice chairperson of the management body to fulfil the roles and responsibilities of the chairperson in the absence of the latter;

(c) an independent member of the management body is appointed senior independent member of the management body;

it is provided that the senior independent member of the management body must not hold the position of the chairperson or the vice-chairperson;

(d) committees of appropriate size, composition, structure and responsibilities are established for the effective discharge of the management body's roles and responsibilities, subject to the provisions of Part IV.

(2) with regards to the organisation of meetings of the management body and its committees:

(a) the management body holds regular meetings to carry out their responsibilities adequately and effectively;

(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 without the chairperson present at least annually to appraise the chairperson's performance;

(e) the arrangement of attending scheduled or special meetings via teleconferencing or videoconferencing must not be abused but used with caution at the member, and management body level ensuring that at least fifty percent (50%) of the management body plus one (1) member, rounded down, of the members are physically present at any scheduled meeting;

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

(g) proxy voting may be permitted for absentees but no more than one (1) proxy vote per each member attending the meeting and members who vote via proxy are held accountable for their proxy vote;

(h) no other person is present unless formally invited to attend for a specific item(s) on the agenda; any such person is present only during the discussion of the specific item and leaves the meeting room immediately after, without any participation in the decision making process.

(3) 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 must 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 must 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 chairperson 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;

it is provided that, a proxy holder must 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 chairperson

must 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 must 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 must 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 must be communicated immediately to the Central Bank.

(4) with regards to the documentation of minutes of meetings of the management body and its committees:

(a) detailed minutes must be kept for each meeting which must 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 must 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 subparagraph 2(h), 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”.

(5) all members of the management body, especially the non-executive members:

(a) receive targeted training for developing and/or refreshing their knowledge and skills; and

(b) have access to the advice and services of the company secretary.

(6) with regards to the treatment of non-compliance with management body policies and procedures -

(a) an appropriate monitoring process is in place for monitoring compliance with management body policies, processes and procedures;

(b) a formal and well documented mechanism is in place for providing instructions and

assigning responsibilities for -

(i) assessing the causes of non-compliances;

(ii) initiating, requesting, implementing and monitoring the effectiveness of corrective measures; and

(iii) documenting the whole procedure and the outcome of the procedure;

(c) communicating in due time non-compliances with the Law and this Directive to the Central Bank, and –

(i) within a month from the date the non-compliance was identified, of the procedure followed and persons involved in resolving these non-compliances; and

(ii) within two (2) months from the date the non-compliance was identified, the remedial / rectification actions taken to address these non-compliances

Access to information and resources of the management body in its supervisory function.

8. (1) The management body in its supervisory function and, where a risk committee has been established, the risk committee must have adequate access to information on the risk situation of the institution and, if necessary and appropriate, to the risk management function and to external expert advice.

(2) The management body in its supervisory function and, where one has been established, the risk committee shall determine the nature, the amount, the format, and the frequency of the information on risk which it is to receive. In order to assist in the establishment of sound remuneration policies and practices, the risk committee shall, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration system take into consideration risk, capital, liquidity and the likelihood and timing of earnings.

Section 2 – Requirements on the nomination, selection and succession of members of the management body and the evaluation of the management body

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

9. (1) The respective nomination committees of institutions must 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 must put in place a policy promoting diversity on the management body.

(2) Institutions must have in place a sound and appropriate recruitment policy for the nomination, selection, reappointment and succession of the members of the management body which must 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 Fitness and Probity Directive of 2014;

(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;

(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) time commitment expected;

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

(e) the term of appointment and the number of re-appointments for executive, non-executive and independent members of the management body;

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

(g) 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 having to be replaced simultaneously.

(3) Institutions must define the maximum number of terms an individual may serve as a non-executive member of the management body; in any case an individual may serve as a non-executive member for a maximum of twelve (12) years including appointments in any management bodies of the group.

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

(5) Institutions must devote adequate human and financial resources to the induction and training of members of the management body.

Evaluation of the management body.

10. (1) Institutions must have in place an appropriate methodology and process for the formal and rigorous evaluation of the performance of the management body as a whole, each committee and each individual member of the management body at least on an

annual basis ; the evaluation process must cover, as a minimum, the following:

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

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

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

(d) communication with management, shareholders and competent authorities;

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

(f) 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 Fitness and Probity Directive of 2014 and particularly the independence of each independent member based on the applicable criteria of the Fitness and Probity Directive of 2014:

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 developments, then the management body must address the issue immediately in accordance with paragraph 7(6) and proceed with the necessary remedial measures, including removing the said member from the management body or redefining his or her role in the management body and/or appointing a new independent member; the time period for implementing all necessary remedial measures should not exceed one (1) month:

It is further provided that the said member should 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) As part of the evaluation process, institutions should ensure that non-executive members of the management body regularly self appraise their individual skills, knowledge and expertise, and determine whether further professional development would help them

develop their expertise and fulfil their obligations.

(3) Institutions must 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 3 – Key roles and responsibilities of the management body

Setting and overseeing strategy.

11.(1) The management body is responsible for setting, periodically reviewing and overseeing the implementation of the institution's business objectives and strategies for achieving those objectives including its risk strategy and internal capital plans, taking into account the institution's long-term financial interests and solvency as well as the interests of depositors, shareholders and other relevant stakeholders.

(2) The management body should ensure that the institution has a blueprint in place for developing business objectives and strategies; this blueprint should ensure that:

(a) the institution's code of business conduct and corporate values are reflected in the business objectives and strategies; and
(b) the roles of the head of the risk management function, the chief financial officer and the treasurer in the development of the strategies are appropriately and clearly differentiated.

(3) In formulating the strategies, the management body should:

(a) set and prioritise the institution's immediate as well as future operational targets both for the institution and the group which it is heading considering the applicable legal and regulatory framework;
(b) establish the risk appetite of the institution through the articulation in written form of a risk appetite statement and risk limits in accordance with paragraph 61 and cascading them through the organisation; and
(c) assess on an ongoing basis and under alternative scenarios in accordance with paragraphs 62(6) and 71(8)-(12), the amounts, types and distribution of internal capital and liquid assets and approve capital and funding plans and a budget commensurate to the type and size of its activities, risk appetite and estimated financial results.

(5) The management body must ensure that the institution has an effective process in place for informing and updating the relevant staff about the institution's strategies in a clear and consistent way.

(6) The management body must establish a process for reviewing the business objectives and strategies on a regular basis, at least annually, to ensure that they remain comprehensive and proportionate to the nature, scale and complexity of the activities of the institution concerned.

(7) The management body must establish a process for evaluating whether the institution is operating within the approved strategies; in this regard the management body must establish and communicate to senior management clear and objective performance goals and measures both for the institution and for senior management

Setting and overseeing the institution and group structure.

12.(1) The management body must understand the institution's structure and the way it's various elements complement and interact with each other, recognise it's limitations, assess the risks that it's limitations and complexity may be causing and guide it's evolution in a way that ensures that the institution structure -

(a) is justified and in line with the approved business strategy and risk appetite of the institution;

(b) does not involve undue or inappropriate complexity that would hinder the ability of the management body to effectively oversee and manage the risks that the institution faces; and

(c) is transparent to its stakeholders.

(2) In case where the institution is the parent undertaking of a group, the management body must -

(a) understand the group structure, the purpose of the group's different units and entities and the links and relationships among them and with the institution; this requires an evaluation of the group-specific operational risks, intra-group exposures and how the group's funding, capital and risk profiles could be affected under normal and adverse circumstances;

(b) keep itself informed about the risks the group's structure may be causing; this includes:

(i) information on major risk drivers; and

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

(c) assess how changes to the group structure, such as new subsidiaries, mergers or acquisitions, suspension of parts of the institution or the group or changes due to external developments, affect its soundness and make any necessary adjustments swiftly.

(3) The management body must approve sound strategies and policies for the

establishment of new structures and ensure that these policies and procedures are communicated to the Central Bank; where an institution or group operates or intends to operate through special purpose vehicles or related structures or in jurisdictions that impede transparency or do not meet international banking standards, these policies must ensure that

(a) such structures and activities -

(i) are accepted only when the associated risks are identified, properly assessed and the institution has satisfied itself that these risks can be appropriately managed or mitigated;

(ii) are subject to appropriate limits;

(b) the need to continue operating through such structures is periodically assessed.

(4) The management body must ensure sound and effective measures and systems are in place for the generation and exchange of information among and about the various units of the institution and in case where the institution is the parent undertaking of a group, the generation and exchange of information among and about the various entities of the group including the type, charter, ownership structure and business of each legal entity.

(5) The management body must ensure that any flow of significant information relevant to the operational functioning of the institution and the group which it is heading is documented and made available to the management body, internal control functions and to the supervisory authorities, including information on approval and maintenance of special purpose vehicles or related structures or in jurisdictions that impede transparency or do not meet international banking standards.

Setting and overseeing the allocation of responsibilities and authority.

13.(1) The management body must ensure there are clear lines of responsibility and accountability throughout the institution, including subsidiaries, affiliated entities and other contractual relations, in line with the operational structure of the institution.

(2) The management body must ensure that a clear and documented allocation of roles, responsibilities and authorities to the management body as a whole, to committees of the management body, to individual members of the management body, to senior management and internal control functions are in place, subject to the provisions of the Law and this Directive, in such a way that:

(a) the allocation of roles, responsibilities and authorities promotes the effective separation between oversight and management function;

(b) it is clear who has which of those roles, responsibilities and authorities;

(c) where responsibilities have been allocated to more than one function, the manner those responsibilities are shared or divided between the functions concerned must

be appropriate and clearly documented;

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

(e) a record of the allocation arrangements is retained for seven (7) from the date on which it was superseded by a more up-to-date record.

(3) The management body must ensure that the allocation of responsibilities to individual members of the management body takes due account of whether the relevant member has the expertise and degree of independence and objectivity required to carry out their allocated functions.

(4) The management body must review and satisfy itself as to the ability of the members of committees to commit appropriate time to the committees; where a committee member is unable to provide sufficient time to attend committee meetings, the management body must replace him or her with a member with appropriate availability, experience and expertise.

(5) The management body must ensure that the heads of the control functions have the authority to carry out their responsibilities and have direct access to the management body.

Setting and overseeing selection and succession of key functions.

14.(1) The management body must establish and oversee the policies for selecting new members of the management body and re-appointing existing members as provided in paragraph 9.

(2) The management body must establish appropriate practices and procedures for monitoring and periodically reviewing:

(a) the adequacy and appropriateness of the size and composition of the management body in accordance with paragraph 6;

(b) the relevant expertise and skill of committee members and their ability to commit appropriate time to the committee;

(c) the fitness and probity of existing members in accordance with the provisions of the Fitness and Probity Directive of 2014.

(3) The management body must establish and oversee the policies for selecting, developing and replacing senior management and heads of internal control functions in accordance with paragraphs 46, 78 and 80.

(4) The management body must establish appropriate practices and procedures for monitoring and periodically reviewing:

(a) the adequacy and effectiveness of the composition and structure of senior

management in accordance with paragraph 45;

(b) the fitness and probity of senior management, in accordance with the provisions of the Fitness and Probity Directive of 2014;

(c) the independence and objectivity of heads of internal control functions.

(5) The management body must approve and periodically review the policy on the recruitment, rotation and promotion of staff.

Overseeing senior management.

15.(1) The management body is responsible for providing effective oversight of senior management; in this regard, it must establish appropriate policies, practices and procedures to ensure that the senior management carries out its roles and responsibilities as provided in paragraphs 47 to 49.

(2) The practices and procedures referred to in subparagraph (1) should include the following:

(a) regular meetings with senior management;

(b) questioning and reviewing critically explanations and information provided by senior management;

(c) setting formal performance goals for senior management consistent with the long-term objectives, strategy and financial soundness of the institution, and monitoring senior management's performance against these goals.

Setting and overseeing code of business conduct and alert procedures.

16.(1) The management body should set the tone at the top for the effective implementation of appropriate standards for professional and responsible behaviour throughout the institution.

(2) The management body must ensure that appropriate and clear policies, process and procedures are in place for -

(a) the implementation and periodical review of a code of business conduct and corporate values, in accordance with paragraph 53; and

(b) monitoring and reporting compliance with these standards and corporate values.

(3) The management body should ensure that the institution establishes appropriate alert procedures enabling employees to communicate potential or actual breaches of internal or regulatory requirements or concerns of wrongdoing within the institution through a specific, independent and autonomous channel without fear of reprisal, in accordance with paragraph 57.

Approving and periodically

17.(1) The management body must approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks the institution is or

reviewing technical criteria for the organisation and treatment of risks.

might be exposed to, including those posed by the macroeconomic environment in which it operates in relation to the status of the business cycle.

(2) The management body must devote sufficient time to 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 in this Directive and in 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 management body shall establish reporting lines thereto that cover all material risks and risk management policies and changes thereof.

(3) The management body has the primary responsibility for establishing, monitoring and assessing the institution's risk culture in accordance with paragraph 60 that ensures a common understanding and awareness of risk, encourages the expression, discussion expression and escalation of concerns on risk to appropriate levels and holds employees at all levels accountable for their actions in relation to the institution's risk taking behaviour; the management body must set the tone at the top by clearly articulating the underlying risk culture values and ensuring their behaviour reflect the values being espoused.

(4) The management body must set and oversee the implementation of the risk appetite framework in accordance with paragraph 61; in this regard, the management body must -

(a) adopt and oversee the implementation of a well documented risk appetite statement;
(b) include an assessment of risk appetite in their strategic discussions including decisions regarding mergers, acquisitions and growth in business lines or products;
(c) regularly and at least every six (6) months, review and monitor actual versus approved risk limits including qualitative measures of risks that are not easy to measure;
(d) satisfy itself that there are mechanisms in place to ensure material adverse risk exposures are effectively managed, and, where necessary, appropriately mitigated, in particular those that are close to risk limits.

(5) The management body must ensure that the institution has an appropriate risk management framework given the institution's business model, complexity and size, which is embedded into the institution's risk culture and in accordance with Part IX; in this regard, the management body shall be actively involved in and ensure that -

(a) risk management objectives, key risk management principles and assignment of risk management responsibilities across all the activities of the institution are clear, well document and consistent with the business objectives and strategies;

(b) external assessments are not used exclusively or mechanistically for risk assessment purposes and that an adequate internal risk assessment capacity is developed, commensurate to the nature, scale and complexity of the institution's activities;

(c) risk management is supported by an adequate and robust management information system to enable identification, measurement, assessment and reporting of risk in a timely and accurate manner;

(d) material changes to the risk management system are documented and subject to approval by the management body;

(e) the development of new markets, products and services offered to customers by any business unit of the institution and significant changes to existing ones are governed by a well documented new product approval policy, in accordance with paragraph 72;

(f) the risk management framework is reviewed regularly to help ensure that necessary modifications and improvements are identified and made in a timely manner.

(5) The management body should adopt and implement a policy on the content, form and frequency of reporting it expects on risks from senior management and internal control functions.

(6) The management body must ensure that the institution evaluates the appropriateness of using internal approaches for calculating own funds requirements on the basis of nature and complexity of the institution's exposures and internal organisation.

Regulatory compliance.

18.(1) The management body must understand the regulatory environment in which the institution operates and ensure that the institution has an appropriate compliance framework in place in accordance with Part VIII and maintains an effective and productive relationship with competent authorities.

(2) The management body must approve the institution's compliance policy referred to in paragraph 59(2)(d) and assess at least once a year the extent to which the institution is managing its compliance risk effectively.

Design and implementation of a sound internal control framework.

19.The management body must ensure that the institution has established an appropriate internal control framework in accordance with Part X; in this regard, the management body must ensure:

(a) the design of internal control systems and the composition of internal control functions are appropriate to the size and complexity of the institution and that these

systems and functions operate effectively and as intended;

(b) for each key business process and policy and related risks and obligations, there are appropriate controls;

(c) all controls and procedures, including the approval procedures, are adequately documented and communicated to the staff responsible for their execution and control;

(d) staff is held accountable for the effective implementation of controls and procedures under their area of responsibility;

(e) at least two members of the staff are directly or indirectly involved in every activity or control function until its completion;

(f) only duly authorised personnel has access to the institution's assets and accounting records and to confidential information in general;

(g) competent persons are appointed to the internal control functions;

(h) internal control functions participate in an advisory capacity in establishing new procedures;

(i) the internal audit function has the capacity to effectively carry out reviews of the risk management framework, the compliance framework and the internal control framework

(j) the internal control framework is assessed by an external auditor in accordance with paragraph 104; in this regard, the management body ensures that it has the same relationship with the external auditor as the one it must have with the approved auditor in accordance with paragraph 22(4).

Setting and overseeing remuneration policy and practices.

20.(1) The management body must adopt and periodically review the remuneration policy in accordance with Part VI and oversee its effective implementation.

(2) The management body must ensure that the remuneration policy and practices are consistent with the risk appetite of the institution, prevent conflicts of interest and promote sound and effective risk management.

Approval of procurement procedures and outsourcing.

21.(1) The management body must ensure that the institution has in place documented procurement procedure for the purchase of products or services, including approval limits; the procurement procedure should ensure that contracts are awarded on the basis of objective criteria which -

(a) ensure compliance with the principles of transparency, non-discrimination and equal treatment; and

(b) guarantee that tenders are assessed in conditions of effective competition.

(2) The management body must approve and regularly, and in any case at least every three (3) years, review the outsourcing policy of the institution and oversee its implementation; the outsourcing policy should be designed and implemented in accordance with the framework of principles on outsourcing, which is outlined in Appendix 2.

Ensuring reliable and transparent financial reporting.

22.(1) The management body must ensure the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with legal and supervisory requirements and relevant standards.

(2) The management body must ensure there is a reliable financial reporting process which is supported by clearly defined roles and responsibilities of the management body, senior management and approved auditor.

(3) The management body must approve and oversee the effective implementation of such systems and controls as necessary to ensure that the financial reports of the institution present a balanced and accurate assessment of the institution's financial position and profitability, in accordance with the International Financial Reporting Standards.

(4) The management body must promote and maintain an effective relationship with the approved auditor by ensuring that:

(a) the terms of engagement of the approved auditor are clear and appropriate to the scope of the audit and resources required to conduct the audit, and specify the level of audit fees to be paid;
(b) the approved auditor undertakes a specific responsibility under the terms of engagement to perform the audit in accordance with applicable international auditing standards;
(c) there are adequate policies and processes to ensure the independence of the approved auditor;
(d) there is adequate dialogue with the approved auditor on the scope and timing of the audit to understand the issues of risk, information on the insurer's operating environment which is relevant to the audit, and any areas in which the management body may request for specific procedures to be carried out by the approved auditor, whether as part or extension of the audit engagement;
(e) there are regular meetings between the management body and the approved auditor during the audit cycle, including meetings without the presence of the senior management;
(f) utilise, in a timely and effective manner, the findings of the approved auditor and

resolve in a timely manner any weaknesses.

Ensuring effective and transparent communication.

23.(1) The management body must ensure that the institution adopts and implements appropriate policies, processes, systems and controls to promote timely and effective disclosures to relevant stakeholders, in accordance with Part X.

(2) The management body must ensure that the financial information and other data submitted to the Central Bank and other competent authorities are –

(a) complete and valid and based on corresponding accounting entries;

(b) in the case of estimates not based on accounting entries, conducted in a proper and appropriately substantiated manner;

(c) submitted within the prescribed time limits.

(3) The management body must oversee the process of disclosure and communication.

Ensuring the implementation of appropriate information security policies, standards and procedures.

24.The management body must ensure that the institution has an appropriate information security framework in place for the protection of the institution's confidential and proprietary information; in this regard it must -

(a) approve and periodically review the institution's information security policy; the information security policy should be laid out in the form of principles and commitments outlining the directions and objectives of the institution for the effective management, protection and allocation of all its information assets, electronic, printed or otherwise;

(b) ensure that appropriate sections of the information security policy are communicated to senior management and staff, on a 'need-to-know' basis, according to their duties and responsibilities;

(c) ensure the institution has an administrative structure in place that oversees the security of operational information;

(d) review reports on the effectiveness of the information security program.

Ongoing monitoring and evaluation of the governance framework.

25.(1) The management body must monitor and periodically assess the effectiveness of the institution's governance arrangements and take appropriate steps to address any deficiencies.

(2) In case where the institution is a parent undertaking of a group, its management body must ensure it has the appropriate means to monitor and assess the governance structure of the group to ensure it remains appropriate in light of growth and increased complexity of the group and complies with all applicable governance requirements, and does so

periodically.

Section 4 –Duties of each member of the management body

Duties of individual members of the management body.

26.(1) Each member of the management body must engage actively in the business of the institution and must be able to make their own sound, informed, objective and independent decisions and judgements to fulfil their individual and collective responsibilities; in this respect, each member of the management body must –

(a) ensure they have a clear understanding of the institution's governance arrangements and their role in them;

(b) ensure they have an up-to-date understanding of the business of the institution including areas for which they are not directly responsible but are collectively accountable;

(c) commit sufficient time to perform their functions in the institution including the preparation of management body meetings;

(d) act with honesty, integrity and independence of mind to effectively assess and challenge the decisions of the senior management where necessary and to effectively oversee and monitor management decision-making;

(e) not use their position to gain undue personal advantage or cause any detriment to the institution;

(f) disclose to the institution any matter that may result, or has already resulted, in a conflict of interest or in a non-compliance with the requirements of the Fitness and Probity Directive of 2014;

(g) ensure their concerns which cannot be resolved about the directing of the institution are recorded in the management body meetings;

(h) acquire, maintain and deepen their knowledge and skills to fulfil their responsibilities.

(2) Executive members of the management body are responsible for proposing strategies to the management body and for executing the agreed strategies to the highest possible standards.

(3) Non executive members of the management body are responsible for monitoring executive activity and contributing to the development of strategies; in this respect, non executive members of the management body should, in addition to the duties provided in subparagraph (1):

(a) constructively challenge and contribute to the development of strategies;

(b) scrutinise the performance of senior management in meeting agreed goals and

objectives and monitor the reporting of performance;

(c) satisfy themselves that financial information is accurate and that the risk and compliance management frameworks and the internal control framework are robust and defensible;

(d) have a prime role in appointing, and where necessary removing, senior management and key personnel in internal control functions, and in succession planning;

(e) have a prime role in establishing and overseeing the remuneration policy referred to in Part VI by the management body;

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

(4) Independent members of the management body must maintain, under all circumstances, their independence of thought and opinion.

(5) Members of the management body must at all times be of sufficiently good repute and possess sufficient knowledge, skills and experience to perform their duties.

Section 5 – Role and responsibilities of the chairperson of the management body

Principal responsibilities of the chairperson of the management body.

27. The principal responsibilities of the chairperson of the management body include the following:

(a) ensuring the effective functioning of the management body;

(b) ensuring that the size and composition of the management body remain appropriate in light of growth and increased complexity of the institution or the group and comply with paragraph 5 and other applicable governance requirements;

(c) ensuring an effective communication with supervisory authorities and stakeholders.

Ensuring the effective functioning of the management body.

28. The chairperson of the management body is responsible for running the management body and ensuring its effectiveness in all aspects of its management and supervisory roles; in this regard, the chairperson is responsible for -

(a) holding management body meetings frequently, in accordance with the applicable provisions of paragraph 7(2);

(b) setting the agenda, taking into account the issues and concerns of all members of the management body;

(c) ensuring that the members of the management body receive accurate, timely and clear information to enable the management body to perform its management and supervisory functions;

(d) ensuring that the members of the management body have sufficient time to consider critical issues and obtain answers to any questions or concerns they may

have and are not faced with unrealistic deadlines for decision making;

(e) encouraging the active participation of members of the management body;

(f) ensuring conflicts of interests are disclosed and members abstain from participating in the decision-making or voting on any matter where they may have a conflict of interest, in accordance with paragraph 7(3);

(g) setting the style and tone of management body discussions to promote effective decision making and constructive debate;

(h) ensuring enough time is allowed for discussion of complex or contentious issues and where appropriate arranging for informal meetings beforehand to enable thorough preparation for the discussion;

(i) ensuring meeting minutes are kept in accordance with paragraph 7(4).

Ensuring the induction, development and performance evaluation.

29.(1) The chairperson of the management body must ensure that members of the management body possess at all times sufficient knowledge and skills to perform their duties; in this regard the chairperson must -

(a) ensure that new members of the management body participate in a full, formal and tailored induction programme, facilitated by the secretaryof the institution;

(b) identify the training needs of the individual members of the management body as well as the management body as a whole to enhance its overall effectiveness as a team and ensure that these needs are met.

(2) The chairperson of the management body must ensure that an evaluation of the management body, its committees and members of the management body individually is carried out in accordance with paragraph 10 and act on the results of such evaluations by recognising the strengths and addressing the weaknesses of the management body.

Ensuring effective communication with supervisory authorities and shareholders.

30.(1) The chairperson of the management body must maintain sufficient contact with the Central Bank and other supervisory authorities and develop an understanding of the views and concerns of major shareholders and investors of the institution.

(2) The chairperson of the management body must ensure that the views and concerns of the Central Bank, other supervisory authorities and major shareholders and investors are communicated to the management body as a whole.

Section 6 – Role and responsibilities of senior independent member of the management body

Roles and respon

31.(1) The duties of the senior independent member of the management body include inter alia the following:

sibilities of the senior independent member of the management body.

(a) to act as a point of contact for shareholders and other stakeholders with concerns which have failed to be resolved or would not be appropriate to go through the normal channels of the chairperson of the management body or senior management;

(b) to ensure that the management body has a balanced understanding of major shareholders issues and concerns.

(c) to chair a meeting with non-executive members of the management body without the chairperson present at least annually in order to appraise the performance of the chairperson in accordance with paragraph 10;

(d) to chair the management body when considering the succession of chairperson of the management body and ensure an orderly succession process.

Section 7 – Roles and responsibilities of the company secretary

Responsibility to appoint a company secretary.

32.(1) Having regard to the provisions of Sections 172 and 173 of the Companies Law, institutions shall take care to avoid any conflict of interest in appointing a company secretary in accordance with Section 171 of the Companies Law.

(2) Notwithstanding the provisions of the Cooperative Credit Institutions Affiliation to a Central Body Directive of 2013 as amended or replaced, cooperative credit institutions shall ensure that a person executes the functions of a company secretary provided in this Section taking due care in order to avoid conflict of interest.

(3) Notwithstanding the provisions of the Companies Law, the company secretary may delegate tasks referred to in this Section to a third person provided there is no conflict of interest and the company secretary checks and signs paperwork and remains responsible and accountable for the outcomes of the delegation;

It is provided that the company secretary may not delegate its tasks to heads of the internal control functions.

Facilitating the functioning of the management body.

33.(1) The company secretary must ensure that 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.

(2) The company secretary must act as a source of information and advice to members of the management body; the company secretary must 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.

(3) The company secretary must ensure that non-executive members have access to independent professional advice at the institution's expense if required, in accordance with paragraph 7.

(4) The company secretary must be closely involved in preparing the schedule of all management body and committee meetings; the company secretary must:

(a) prepare the agendas for these meetings in conjunction with the chairperson 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.

(5) The company secretary must ensure minutes are kept in accordance with paragraph 7; the company secretary must –

(a) express explicitly, in a separate paragraph, his or her 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.

(6) The company secretary must provide support to the management body in setting succession planning and overseeing succession and rotation of tasks of non-executive members of the management body.

Facilitating the induction, development and evaluation of members of the management body.

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

(2) The company secretary must assist the chairperson 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.

(3) The company secretary must provide assistance and support the chairperson in

developing and performing performance evaluations of the management body as a whole, its committees and individual members in accordance with paragraph 10.

PART IV
COMMITTEES OF MANAGEMENT BODY

Section 1 – General requirements

Requirement to establish committees.

35.(1) Institutions must establish management body committees that are appropriate to the size, internal organisation and the nature, scope and complexity of their activities.

(2) Institutions are required to establish a risk committee, a nomination committee and a remuneration committee.

It is provided that institutions must also establish an audit committee referred to in Section 46 of the Auditors and Statutory Audits of Annual and Consolidated Accounts Law of 2009.

(3) The Central Bank may allow an institution which is not considered significant in terms of its size, internal organisation and nature, scope and complexity of its activities to combine the risk committee with the audit committee and/or the nomination committee with the remuneration committee; members of a combined committee shall have the knowledge, skills and expertise required for the committees is composed of.

(4) The Central Bank may allow an institution which is a subsidiary of a group and is not considered significant in terms of its size, internal organisation and nature, scope and complexity of its activities not to establish a remuneration committee or a nomination committee provided that the relevant duties are performed by the respective committees of the parent company and submit their recommendations and decisions to the management body of the institution,

(5) Institutions must communicate the composition of management body committees to the Central Bank within one (1) month of their set up or of change of the composition.

Composition and organisation of committees.

36.(1) The committees of the management body shall comply with the following regarding their composition:

(a) the number of members of committees must be sufficient, and in all cases not less than three (3) members, to handle the size and complexity of their functions;

(b) more than fifty percent (50%), of the committee members must be independent members;

(c) the committees referred to in paragraph 35(2) shall be composed of members of

the management body who do not perform any executive function in the institution concerned;

(d) committee members must not hold any other posts or positions or conduct transactions which could be considered to be in conflict with the terms of reference of the committee;

(e) cross committee membership must ensure that no individual exercises excessive influence or control; in any case, a member of the management body must not be member of more than two (2) committees referred to in paragraph 35(2).

(2) The committees must report regularly to the management body and they must circulate their minutes to the management body in advance of management body meetings.

(3) The management body must establish a process for the co-ordination and communication among its different committees.

(4) Institutions must ensure that the committees have adequate access to the internal control functions and to external expert advice and that the heads of the internal control functions are invited regularly in the meetings of their respective committee.

(5) The chairperson of each committee must ensure that no other person is present, including other members of the management body, unless formally invited to attend for a specific item(s) on the agenda; any such person is present only during the discussion of the specific item and leaves the meeting room immediately after, without any participation in the decision making process.

Terms of reference of committees.

37.(1) The authority, duties, membership, organisation, procedures and reporting lines of each committee must be described and documented by the management body, in accordance with the requirements of this Part and paragraph 7.

(2) The terms of reference must be reviewed regularly, at least annually, by each committee to ensure continuing appropriateness; the reviews must be documented and include, where necessary, recommendations to the management body on revisions.

Section 2 – Audit Committee

Audit committee membership eligibility criteria.

38.(1) The audit committee as a whole should have -

(a) recent and relevant practical experience in the area of financial markets or professional experience directly linked to financial markets activity;

(b) knowledge of the institution's broader business environment including information systems and technology.

(2) The chairperson of the audit committee must be independent and have specialist knowledge and experience in the application of accounting principles and internal control processes.

(3) The chairperson of the management body may not be a member of the audit committee.

(4) Audit committee meetings, where appropriate, must coincide with important financial reporting dates.

Duties of the audit committee.

39. The duties of the audit committee should include the following:

(a) the monitoring and assessment, on an annual basis, of the adequacy and effectiveness of internal control and information systems, based on reports from the internal audit function and the observations and comments of external auditors and competent supervisory authorities and subsequently the submission of proposals to the management body for addressing any weaknesses which have been identified;

(b) the submission of proposals to the management body on the appointment, compensation, terms of engagement and substitution or rotation of the approved auditor and other external auditors;

(c) the liaison with external auditors particularly in relation to their audit findings;

(d) the assessment and monitoring of the independence adequacy and effectiveness of internal audit function;

(e) advising the management body, drawing on the work of the compliance function, on the adequacy and effectiveness of the framework for business conduct;

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

(g) the assessment and monitoring of the independence, adequacy and effectiveness of the compliance function or in the case where the tasks of the compliance function are carried out by a combined control function in accordance with paragraph 76(1), the assessment and monitoring of the independence, adequacy and effectiveness of the combined control function in carrying out the tasks of the compliance function;

(h) subject to paragraph 41(j), the submission to the management body of recommendations for the appointment or removal of the head of the internal audit function and compliance function;

(i) subject to paragraph 41(k), the annual appraisal of the heads of the internal audit function and compliance function and subsequently their submission to the

management body;

(j) the review and approval of the annual audit plan of the internal audit function and the compliance programme of the compliance function,

(k) the review and approval of the budgets of the internal audit function and compliance function, ensuring that they are sufficiently flexible to adapt to variations in response to developments;

(l) the oversight that senior management takes the necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations and other weaknesses identified by external auditors, the internal audit and compliance functions and supervisory authorities;

(m) the monitoring of the establishment of accounting policies and practices;

(n) the monitoring of the financial reporting process and the integrity, accuracy and reliability of the institution's financial statements and any formal announcements relating to the institution's financial performance;

(o) the carrying out of a self-assessment and reporting its conclusions and recommendations for improvements and changes to the management body.

Section 3 – Risk Committee

Risk committee membership eligibility criteria.

40. Members of the risk committee must have appropriate knowledge, skills and expertise to fully understand and monitor the risk strategy and the risk appetite of the institution.

Duties of the risk committee.

41. (1) Without prejudice to the overall responsibility of the management body for risks, the risk committee shall:

(a) advise the management body on the institution's overall current and future risk appetite and strategy, taking into account -

(i) the requirements set out in this Directive;

(ii) the financial and risk profile of the institution; and

(iii) the capacity of the institution to manage and control risk;

(b) assist the management body in overseeing the effective implementation of the risk strategy by senior management including -

(i) the development of mechanisms to ensure material exposures that are close to, or exceed approved risk limits are managed and, where necessary, mitigated in an effective and timely manner;

(ii) the identification and escalation of breaches in risk limits and of material risk

exposures in a timely manner;

(c) review whether prices of liabilities and assets offered to clients take fully into account the institution's business model and risk strategy; where prices do not properly reflect risks in accordance with the business model and risk strategy, the risk committee shall present a remedy plan to the management body;

(d) in order to assist in the establishment of sound remuneration policies and practices, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration system take into consideration risk, capital, liquidity and the likelihood and timing of earnings;

(e) submit to the management body proposals and recommendations for corrective action, whenever weaknesses are identified in implementing the risk strategy;

(f) assess and monitor the independence, adequacy and effectiveness of the risk management function and information security function;

(g) advise the management body, drawing on the work of the audit committee, risk management function and external auditors, on the adequacy and effectiveness of the risk management framework;

(h) advise the management body, drawing on the work of the audit committee, information security function and external auditors, on the adequacy and effectiveness of the information security framework;

(i) advise the management body, drawing on the work of the audit committee, risk management function and information security functions and external auditors, on the adequacy and robustness of information and communication systems to -

(i) enable identification, measurement, assessment and reporting of risk in a timely and accurate manner;

(ii) ensure the adequate protection of the institution’s confidential and proprietary information;

(j) submit to the management body recommendations for the appointment or removal of the heads of the risk management function and information security function;

(k) carry out the annual appraisal of the heads of the internal risk control, compliance and information security functions and submitting it to the management body;

it is provided that, in case where the institution has combined the compliance function with the risk management function in accordance with paragraph 76(1), the risk committee shall carry out this task drawing on the assessment by the audit committee of the role of the head of the combined internal control function on the adequacy and effectiveness of the combined control function in carrying out the tasks of the compliance function;

(l) the review and approval of the budgets of the risk management function and

information security functions, ensuring that they are sufficiently flexible to adapt to variations in response to developments;

(m) advise the management body, drawing on the work of the audit committee, risk management function and external auditors, on the adequacy of provisions and effectiveness of strategies and policies with respect to maintaining, on an ongoing basis, amounts, types and distribution of both internal capital and own funds adequate to cover the risks of the institution;

(n) conduct a self assessment and reporting its conclusions and recommendations for improvements and changes to the management body.

(2) The risk committee must determine the nature, the amount, the format, and the frequency of the information which it is to receive on the risk situation of the institution and for each type of risk and each business unit; the risk committee must -

(a) approve metrics or a process to satisfy itself that the risk reports and information they receive are accurate, comprehensive and depicts an appropriate view of the institution's risk profile;

(b) ensure that risk parameters and risk models developed and used to quantify them are subject to periodic independent validation.

Section 4 – Remuneration Committee

Remuneration committee membership eligibility criteria.

42. The remuneration committee must 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.

Duties of the remuneration committee.

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

(2) When preparing the decisions referred to in subparagraph (1), the remuneration committee must take into account the long-term interests of shareholders, investors and other stakeholders in the institution and the public interest and ensure that:

(a) these are closely linked with the institution's business objectives and strategies;

(b) these are in line with the requirements set out in Part VI;

(c) non-executive members are not included in the beneficiaries of performance

related remunerations.

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

(4) The remuneration committee must ensure that staff members who are involved in the design, review and implementation of the remuneration policies and practices have relevant expertise and are capable of forming independent judgement on the suitability of the remuneration policies and practices, including their suitability for risk management.

(5) The remuneration committee must conduct a self assessment and report its conclusions and recommendations for improvements and changes to the management body.

Section 5 – Nomination Committee

Duties of the nomination committee.

44.(1) The main duties and responsibilities of the nomination committee, inter alia, 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;

(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 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;

(h) conducting an annual self assessment and reporting its conclusions and recommendations for improvements and changes to the management body.

(2) For the purposes of subparagraph (1)(a), the nomination committee must 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 must be made public in accordance with Article 435(2)(c) of Regulation (EU) No 575/2013.

(3) In performing its duties, the nomination committee must, 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 institution as a whole.

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

PART V
SENIOR MANAGEMENT

Composition of senior management.

45.(1) Subject to Section 19 of the Law, senior management must be of sufficient size and expertise to effectively direct the operations of the institution.

(2) Institutions must 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.

46.(1) Institutions must have appropriate policies and procedures in place for selecting, developing and, when appropriate, replacing the chief executive 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 institution and its group; these policies, plans and procedures must 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 and other senior managers and heads of

internal control functions in carrying out their duties and responsibilities;

(ii) conformity with regulatory requirements;

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

(c) the succession planning for chief executive 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 organisation;

(d) 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 senior management.

47.(1) The chief executive and other senior managers are responsible for directing and overseeing the effective management of the 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) overseeing the operations of the institution and providing direction to it on a day-to-day basis, 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 institution and providing direction on a day-to-day basis.

48.(1) Senior management is responsible for implementing an effective and transparent operational structure in the institution or the group, consistent with business objectives, strategies and policies approved by the management body; where the institution has overseas operations or operates through special purpose vehicles or other structures or in jurisdictions that impede transparency, the senior management should exercise adequate oversight of the 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

is accessible to the management body and 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 must oversee the exercise of such delegated responsibility.

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

(5) Senior management must 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.

(6) Senior management must implement an appropriate compliance framework consistent with the direction given by the management body and in accordance with Part VIII.

(7) Senior management must 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 IX; senior management must ensure that a new products approval policy is developed and effectively implemented in accordance with paragraph 72.

(8) Senior management must implement an appropriate internal control framework consistent with the direction given by the management body and in accordance with Part X; the senior management must ensure that sufficient resources with appropriate authority and expertise are dedicated to internal control functions.

(9) Senior management must ensure that the institution develops appropriate information and communication systems to help the management body and senior management to provide effective oversight of the institution consistent with the direction given by the management body and in accordance with Part XI; senior management is responsible for ensuring that appropriate records are kept in accordance with paragraphs13, 62 and 0.

(10) Senior management must set appropriate human resource policies including management development and succession planning.

Providing the management body with recommendations.

49.(1) Senior management must 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 must 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 must report to the management body weaknesses and identified limitations of strategies and plans with remediation recommendations.

PART VI
REMUNERATION FRAMEWORK

Remuneration policies.

50.When establishing and applying the total remuneration policies, inclusive of salaries and discretionary pension benefits, for categories of staff including senior management, risk takers, staff engaged in internal control functions and any employee receiving total remuneration that takes them into the same remuneration bracket as senior management and risk takers, whose professional activities have a material impact on their risk profile, institutions must comply with the following principles in a manner ad to the extent 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 institution;

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

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

(d) 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;

(e) 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;

(f) the remuneration of the senior officers in the control risk function is directly overseen by the remuneration committee referred to in subparagraph (2) of paragraph 35 or by a combined nomination and remuneration committee in accordance with subparagraph (3) of that paragraph;

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

(i) basic fixed remuneration, which should 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 should 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.

(2) Institutions must ensure that shareholders are informed of the total remuneration of senior management.

(3) For the purposes of this paragraph, institutions shall comply with the EBA guidelines on remuneration policies and practices of 2010 as amended or replaced.

Variable elements of remuneration.

51. For variable elements of remuneration, the following principles shall apply in addition to, and under the same conditions as, those set out in paragraph 50:

(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 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 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 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) 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 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:

- the shareholders or owners or members of the institution shall act upon a detailed recommendation by the 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;
- shareholders or owners or members of the 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;
- the institution shall notify all shareholders or owners or members of the institution, providing a reasonable notice period in advance, that an approval under the first subparagraph of this point will be sought;
- the institution shall, without delay, inform Central Bank 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 Central Bank that the proposed higher ratio does not conflict with the institution's obligations under this Directive and under Regulation (EU) No 575/2013, having regard in particular to the institution's

own funds obligations;

- the institution shall, without delay, inform the Central Bank of the decisions taken by its shareholders or owners or members, including any approved higher maximum ratio pursuant to the first subparagraph of this point, and the competent authorities shall use the information received to benchmark the practices of institutions in that regard;
- 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 institution;

(iii) 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; institutions that opt to apply the provisions of this point, must comply with the EBA guidelines on the applicable notional discount rate for variable remuneration of 2014 as amended or replaced.

(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 must align with the long-term interests of the 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 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, subject to the legal structure of the institution concerned or share- linked instruments or equivalent non-cash instruments, in the case of a non-listed institution;

(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 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 institution. Central Bank 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) 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 member of staff in question.

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 member of staff in question;

(n) the variable remuneration, including the deferred portion, is paid or vests only if it is sustainable according to the financial situation of the institution as a whole, and justified on the basis of the performance of the 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 institution occurs, taking into account both current remuneration and reductions in payouts of amounts previously earned, including through malus or clawback arrangements.

Up to one hundred percent (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 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 institution.

If the employee leaves the institution before retirement, discretionary pension benefits shall be held by the institution for a period of five years in the form of

instruments referred to in point (l). 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.

Institutions that benefit from government intervention.

52. In the case of institutions that benefit from exceptional government intervention, the following principles shall apply in addition to those set out in paragraph 50:

(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 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 institution;

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

PART VII
FRAMEWORK FOR BUSINESS CONDUCT

Corporate values and code of business conduct.

53. (1) Institutions must develop, approve and promote throughout the organisation a code of business conduct and corporate values on the basis of generally acceptable principles.

(2) The institution's code of business conduct and corporate values should articulate acceptable and unacceptable behaviours; such code and values should clearly disallow behaviour that could result in the institution engaging in any improper, unethical or illegal activity, such as financial misreporting, money laundering, fraud, bribery or corruption and discourage the taking of excessive risks as defined by internal corporate policy.

(3) The code of business conduct and corporate values should include among other due diligence, effectiveness, responsibility, due relationship with members of the public, non-application or acceptance of benefits which are not of a token value and the implementation of professional confidentiality.

Services offered to

54. Institutions must establish appropriate policies, practices and procedures for the fair, honest and professional treatment of customers; in this respect, institutions must, as a

customers. minimum:

(a) adopt best practices for offering services and products which are best suited to customers;

(b) monitor and assess the manner of servicing customers and, especially, the contract terms offered, which should be in conformity with the provisions of the consumer protection laws which are in force from time to time;

(c) establish and operate a suitable complaints procedure to be utilised by customers;

(d) safeguard the interests of customers by offering protection against the misuse of their personal data, in accordance with the provisions of the Processing of Personal Data (Protection of Individuals) Law of 2001.

Conflicts of interest and segregation of duties.

55.(1) Institutions must establish, implement and maintain effective conflict of interest policies for the identification, prevention and management of conflicts of interests.

(2) The conflict of interest policies should identify the relationships, services, activities or transactions in which conflicts of interest may arise; these policies should cover relationships -

(a) between the institution and its stakeholders, including:

(i) its customers;

(ii) its shareholders;

(iii) the members of its management body;

(iv) its staff;

(v) significant suppliers or business partners; and

(vi) other related parties, such as its parent undertaking or subsidiaries; and

(b) between different clients of an institution.

(3) The conflict of interest policies should set out measures to be adopted to prevent or manage conflicts of interest; such procedures and measures should include:

(a) adequate segregation of duties, entrusting conflicting activities within the chain of transactions or of services to different persons or entrusting monitoring and reporting responsibilities for conflicting activities to different persons;

(b) establishing information barriers such as physical separation of certain departments;

(c) preventing persons who are active outside the institution from having inappropriate influence within the institution regarding conflicting activities;

(d) in the case of a parent institution, considering and balancing the interests of all of its subsidiaries, considering how these interests contribute to the common purpose and interests of the group as a whole over the long term.

(4) Conflicts of interest that have been disclosed to and approved by the management body shall be appropriately managed.

Non-standard or non-transparent activities.

56. Institutions must establish and implement effective policies and procedures in accordance with paragraph 73 for –

(a) approving and operating through special-purpose or related structures or in jurisdictions that impede transparency or do not meet international banking standards;

(b) approving and performing non-standard or non-transparent activities for customers.

Alert procedures.

57. (1) Institutions must adopt appropriate alert procedures in order to encourage employees to communicate internally through a specific, independent and autonomous channel, or to the Central Bank -

(a) potential or actual breaches of -

(i) laws or regulations;

(ii) internal policies, standards and procedures;

(b) concerns about unethical and questionable practices,

(c) serious irregularities and omissions;

(2) The procedures referred to in subparagraph (1) shall include at least:

(a) appropriate protection for employees who report breaches against retaliation, discrimination or other types of unfair treatment;

(b) protection of personal data concerning both the employee who reports the breaches or concerns and the person who is allegedly responsible for a breach in accordance with the Processing of Personal Data (Protection of Individuals) Law of 2001;

(c) clear rules that ensure that confidentiality of the employees that reports breaches or concerns is guaranteed at all times by providing the opportunity to raise such concerns outside regular reporting lines;

(d) employees to have the option to submit their concerns anonymously

(e) autonomous channel to communicate material breaches or concerns directly to the management body, or the Central Bank.

PART VIII
COMPLIANCE FRAMEWORK

Compliance culture.

58. (1) Institutions shall develop an integrated and institution-wide compliance culture, -

(a) 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 risk are managed; and

(b) in line with their code of business conduct and corporate values;

institutions should develop their compliance culture through policies, examples, communication and training of staff regarding their responsibilities for compliance.

(2) 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 work.

Requirement to establish a compliance framework.

59.(1) Institutions must design, develop and implement an integrated institution-wide compliance framework set by a compliance policy and supported by compliance plans, processes and assurance.

(2) Institutions must ensure that their compliance framework includes as a minimum the following aspects:

(a) a compliance policy setting out the business and legal environment applicable to the institution and objectives, principles and allocation of responsibilities for compliance; in group structures, compliance policy must address the manner compliance responsibilities are allocated and carried out on group and entity level;

(b) processes and procedures for establishing and maintaining an updated register of internal, regulatory and business requirements, the obligations that each set of requirements imposes and links to the policies and procedures developed by the institution to address these obligations;

(c) processes and procedures for identifying, assessing, managing and monitoring risks of non-compliance with these obligations;

(d) mechanism for reporting and handling breaches and incidents;

(e) key personnel responsible for coordinating and monitoring compliance;

(f) guidance, support, and training available to assist staff in meeting its obligations.

(3) Institutions must ensure that their compliance identification process covers the following

areas of compliance:

(a) institution's code of business conduct and corporate values;
(b) prudential laws and regulations;
(c) regulations on the prevention of money laundering and terrorist financing;
(d) regulations on 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.

(4) Institutions must ensure that their compliance monitoring processes and procedures include the submission of regular reports to the compliance function by staff appointed as compliance officers at major business units, branches and subsidiaries in the Republic and abroad to perform compliance tasks and assist the compliance function to discharge its tasks.

PART IX
FRAMEWORK FOR THE TREATMENT OF RISK

Section 1 – Risk culture and risk appetite

Risk culture.

60.(1) Institutions shall develop an integrated and institution-wide risk culture, based on a full understanding of the risks they face and how they are managed, in line with their risk appetite; institutions should develop their risk culture through policies, examples, communication and training of staff regarding their responsibilities for risk.

(2) Institutions shall ensure that the risk culture is appropriately disseminated at all hierarchical levels, with the objective of raising awareness and ensuring that each member of staff -

(a) understands the nature of every risk associated with the discharge of its operational or supervisory duties and the need and responsibility for managing these risks; and
(b) understands the importance of internal control functions in risk management and facilitates their implementation.

Risk appetite framework.

61.(1) Institutions shall ensure that an effective risk appetite framework is in place through appropriate policies, processes, controls, and systems for senior management and management body to communicate, understand and assess the aggregate level of risk and types of risk the institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan.

(2) An effective risk appetite framework requires as a minimum:

(a) assessing the risk capacity of the institution;
(b) establishing the risk appetite of the institution through the articulation in written form of a risk appetite statement;
(c) allocating the 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 institution against its risk appetite;
(e) an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the risk appetite framework.

(3) Institutions shall ensure that the risk appetite statement:

(a) is linked to the institutions' strategic, capital and financial plans, as well as compensation programs;
(b) establishes the amount of risk the 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 operation the maximum level of risk that the institution is willing to operate within, based on its risk appetite, risk capacity, and risk profile;
(d) includes quantitative measures that can be translated into risk limits applicable to business lines and units which in turn can be aggregated and disaggregated to enable measurement of the risk profile against risk appetite and risk capacity;
(e) includes qualitative statements for risks that are not easy to measure, including reputational and financial consequences of poor management of conduct risks across retail and wholesale markets, and establish some form of boundaries or indicators to enable monitoring of these risks;
(f) ensures that the strategy and risk limits of each business line and legal entity align with the institution-wide risk appetite statement as appropriate; and
(g) is forward looking and subject to scenario and stress testing to ensure that the institution understands what events might push the institution outside its risk appetite and/or risk capacity.

(4) Institutions shall ensure that risk limits:

(a) are set at a level to constrain 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 institution-wide, business line and business unit levels such as counterparty, industry, region, collateral type, currency and product;
(c) are monitored regularly.

(5) Institutions shall ensure that the necessary mechanisms are in place to make the risk appetite framework adaptable to changing business and market conditions.

(6) Institutions should ensure breaches of risk limits are escalated and addressed with appropriate follow up.

Section 2 – Risk management framework

Subsection 2.1 – General requirements

General requirements on risk management.

62.(1) Institutions must ensure that an appropriate and holistic risk management framework is in place to enable them to make risk aware decisions -

(a) extending across all their business, support functions and control units,
(b) recognizing fully the economic substance of their risk exposures, and
(c) encompassing all relevant risks, financial and non-financial, on and off balance sheet, and whether or not contingent or contractual.

(2) The risk framework must ensure that all material risks including the risks referred to in paragraphs 63 to71, are identified and managed; institutions shall ensure that appropriate, adequate and effective policies, systems, processes and procedures are in place for:

(a) identifying all relevant risks to the institution, on a continuous basis, current and emerging, at the transaction and portfolio levels;
(b) assessing these risks and measuring the institution's exposures to them, at the transaction and portfolio levels, on an individual basis and on an integrated basis by recognising interactions between these risks, in an accurate and timely manner;
(c) monitoring the risk exposures and determining the corresponding capital needs on an ongoing basis;
(d) monitoring and assessing decisions to accept particular risks, risk mitigation measures and whether risk decisions are in line with the risk appetite and risk limits;

(e) reporting to the senior management and the management body as appropriate, on all the aforementioned;

(f) keeping appropriate records.

(3) Institutions shall ensure that each material risk is associated with a policy, process or measure as well as a control to ensure that any such policy, process or other measure is being applied and works as intended.

(4) Assessment of risks must not solely or mechanistically rely on external assessments such as external credit ratings or purchased risk models but institutions should strive to develop internal assessment capacity commensurate to the size, nature and scale of their activities; institutions must ensure that purchased risk models are validated and calibrated to the institution's individual circumstances to ensure accurate and comprehensive capture and analysis of its risk profile and risk capacity.

(5) Risks shall be evaluated bottom up and top down, at the institution-wide, business line and business unit levels, using consistent terminology and compatible methodologies throughout the institution and its group.

(6) Institutions must use forward looking tools such as scenario analysis and stress tests as part of their risk identification and measurement processes in order to identify potential risk exposures under a range of adverse circumstances; for the purposes of this subparagraph, institutions must:

(a) identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to their business and risk profile and consider their exposures to those circumstances, including:

(i) circumstances and events occurring over a protracted period of time;

(ii) sudden and severe events, such as market shocks or other similar events; and

(iii) some combination of the circumstances and events described in (i) and (ii), which may include a sudden and severe market event followed by an economic recession;

(b) estimate the financial resources that it would need in order to continue to meet the capital requirements laid down in Regulation (EU) 575/2013 under the adverse circumstances being considered;

(c) assess how risks aggregate across business lines or units, any material non-linear or contingent risks and how risk correlations may increase in stressed conditions;

(d) document and test assumptions and limitations of such tools.

(7) The risk management framework shall ensure that decisions which determine the level

of risk taken do not exclusively rely on quantitative information or model outputs, but take into account the practical and conceptual limitations of metrics and models using a qualitative approach such as expert judgement and critical analysis; institutions shall ensure that assessments of the impact of relevant macroeconomic environment trends and data on exposures and portfolios are formally integrated into material risk decisions.

(8) Institutions shall ensure that backward looking tools are used to review their actual risk profile against the institution's risk appetite and risk limits and provide input for any adjustment.

(9) Institutions must establish reporting lines to the management body that cover all material risks and risk management policies and changes thereof.

(10) Institutions must ensure that regular and transparent reporting mechanisms are established so that the management body and all relevant functions -

(a) are provided with reports in a timely, accurate, concise, understandable and meaningful manner; and
(b) can share relevant information about the identification, measurement or assessment and monitoring of risks.

(11) Institutions must make a written record on a solo 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 analyses 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.

Subsection 2.2 – Treatment of specific risks

Credit and counter party risk.

63. (1) Institutions must lay down sound and well-defined credit-granting criteria and must 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 2013 and the Arrears Management Directive of 2013 to 2014.

(2) Institutions must have internal methodologies that:

(a) enable them to assess the credit risk of exposures to individual obligors, securities or securitisation positions and credit risk at the portfolio level;
(b) do not rely solely or mechanistically on external credit ratings; and
(c) 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, do not exempt the institutions from additionally considering other relevant information for assessing its allocation of internal capital.

(3) Institutions must establish effective systems to operate 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.

(4) Institutions must establish appropriate systems for the effective management of credit facilities in arrears and the conduct of feasible and sustainable debt restructurings in accordance with the provisions of the Arrears Management Directive of 2013-2014.

(5) Institutions must adequately diversify credit portfolios given an institution's target markets and overall credit strategy.

Residual risk.

64. Institutions must address and control, including by means of written policies and procedures, the risk that recognised credit risk mitigation techniques used by them prove less effective than expected.

Concentration risk.

65. Institutions must address and control, including by means of written policies and procedures, the concentration risk arising from:

(a) 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;

(b) the application of credit risk mitigation techniques; and

(c) risks associated with large indirect credit exposures such as a single collateral issuer.

Securitisation risk.

66. (1) Institutions must evaluate and address through appropriate policies and procedures, the risks arising from securitisation transactions in relation to which an 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) An 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.

67.(1) Institutions must 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) Institutions must implement policies and processes 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) Institution's must 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) 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, must 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; 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) Institutions must 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.

68. Institutions must implement systems to identify, evaluate and manage the risk arising from potential changes in interest rates that affect an institution's non-trading activities.

Risk of excessive leverage.

69.(1) Institutions must have in place policies and procedures 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) Institutions must 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 institution's own funds through expected or realised losses, depending on the applicable accounting rules; to that end, institutions must be able to withstand a range of different stress events with respect to the risk of excessive leverage.

Operational risk.

70.(1) Institutions must implement policies and processes to evaluate and manage the exposure to operational risk, including model risk, and to cover low-frequency high severity events; institutions must articulate what constitutes operational risk for the purposes of those policies and procedures.

(2) Institutions must have in place contingency and business continuity plans to ensure the institution's ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Liquidity risk.

71.(1) Institutions must 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 institutions and risk tolerance set by the management body and shall reflect the institution's importance in the Republic and in any other Member State in which it carries out business. Institutions shall communicate risk tolerance to all relevant business lines.

(3) Institutions, taking into account the nature, scale and complexity of their activities, shall have liquidity risk profiles that are consistent with and, not in excess of, those required for a well-functioning and robust system.

(4) Institutions must 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.

(5) Institutions must distinguish between pledged and unencumbered assets that are available at all times, in particular during emergency situations; institutions must 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 must monitor how assets can be mobilised in a timely manner.

(6) Institutions must 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.

(7) Institutions must 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; institutions must ensure that these arrangements are reviewed regularly.

(8) Institutions must 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 must 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 institution acts as sponsor or provides material liquidity support.

(9) Institutions must consider the potential impact of institution-specific, market-wide and combined alternative scenarios; different time periods and varying degrees of stressed conditions must be considered.

(10) Institutions must 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).

(11) Institutions must 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; Those plans must be tested, 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 management body so that internal policies and processes can be adjusted accordingly; institutions must take the necessary operational steps in advance to ensure that liquidity recovery plans can be implemented immediately.

(12) The operational steps referred to in subparagraph (11) must include holding collateral immediately available for central bank funding; this includes holding collateral where necessary in the currency of another member state, or currency of a third country to which the 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.

Subsection 2.3 – New products and markets and non standard or non transparent activities.

New products and markets.

72.(1) An institution shall have in place a well-documented new products approval policy, approved by the management body, which addresses the development of new markets,

products and services and significant changes to existing ones.

(2) An institution's new products approval policy should 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; the new products approval policy should also include the definitions of "new product", "new market" and "new business" to be used in the organisation and the internal functions to be involved in the decision-making process.

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

(4) The new products approval policy should ensure that decisions to launch a new activity clearly state the business unit and individuals responsible for it; a new activity should not be undertaken until adequate resources to understand and manage the associated risks are available.

(5) Institutions must ensure that the risk management function and compliance function express an opinion prior to entering in new markets, introducing new products and services and making significant changes to existing ones.

Non standard or non transparent activities.

73.(1) Institutions must develop and effectively implement adequate policies and procedures and documented processes for the approval and maintenance of special purpose vehicles or related structures or in jurisdictions that impede transparency or do not meet international banking standards to ensure -

(a) associated risks are appropriately identified and managed; and

(b) the continuing need to perform such activities is periodically assessed to ensure such structures and activities remain consistent with their intended aim.

(2) Institutions must develop and effectively implement similar policies, procedures and processes when performing non-standard or non-transparent activities for clients, in accordance with the Prevention and Suppression of Money Laundering Activities Law of 2007 and the CBC Directives and circulars for the prevention of money laundering and terrorist financing issued in accordance with article 59(4) of the said Law.

PART X
INTERNAL CONTROL FRAMEWORK

Section 1 – General requirements

Requirement to establish an internal control framework.

74.(1) Institutions must design, develop and maintain a strong and comprehensive internal control framework, including a system of controls and independent internal control functions with appropriate standing to fulfil their mission.

(2) The design of the internal control framework should ensure -

(a) effective and efficient operations;

(b) adequate control of risks;

(c) prudent conduct of business;

(d) effective separation between oversight and business functions;

(e) reliability of financial and non-financial information reported, both internally and externally; and

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

(3) The internal control framework should -

(a) cover the whole organisation, including the activities of all business, support and control units;

(b) be appropriate for an institution's business, with sound administrative and accounting procedures.

(4) In developing its internal control framework, an institution should ensure there is a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority to ensure compliance with internal rules and decisions; the business and support units should have the primary responsibility for establishing and maintaining adequate internal control policies and procedures with the possible participation of internal control functions in an advisory capacity.

(5) An appropriate internal control framework requires verification by independent internal control functions that these policies and procedures are complied with.

Section 2 – Internal control system

Requirement to establish a system of controls.

75.Institutions shall design and operate an effective system of internal controls that is appropriate to the nature, scale, and complexity of the institution's business and risk profile; institutions must ensure that their internal control system includes as a minimum the following aspects:

(a) appropriate controls to ensure that all transactions are -

(i) duly authorised and legal;

(ii) executed in accordance with all relevant procedural rules of each operational unit;

(iii) assessed as to their inherent risk;

(iv) carried out by duly authorised and immediately identifiable persons;

(v) duly recorded in the relevant books and records;

(vi) duly entered into the management information system;

(b) appropriate controls to provide reasonable assurance over the fairness, accuracy, and completeness of the institution's books, records, and accounts, and over financial consolidation and reporting;

(c) appropriate controls for other key business procedures and policies, including for major business decisions and transactions, critical IT functionalities, access to databases and IT systems by employees, and important legal and regulatory obligations;

(d) appropriate controls for the sound and effective operation of information technology systems;

(e) appropriate segregation of duties where necessary, and controls to ensure such segregation is observed;

(f) controls at the appropriate levels so as to be effective, including at the procedure or transactional level and at the business line/unit level;

(g) a minimum absence of two consecutive weeks per year of employees in sensitive positions such as wire transfer operations; during their absence -

(i) their remote electronic access to systems or records from must be denied;

(ii) their daily work should be processed by another employee;

(h) a centralised written inventory of key procedures and policies institution-wide, and of the controls in place in respect of such procedures and policies;

(i) training in respect of controls, particularly for employees in positions of high responsibility or who carry out high risk activities;

(j) procedures for regularly checking that the totality of all controls forms a coherent system and that this system works as intended, fits properly within the overall governance structure of the institution, and provides an element of risk control that complements the risk identification, risk assessment, and risk management activities of the institution;

(k) periodic testing and assessments to determine the adequacy, completeness, and effectiveness of the internal control system and its utility to the management body and senior management for controlling the operations of the institution.

Section 3- Internal control functions

Subsection 3.1 – General requirements for control functions

Requirement to establish internal control functions.

76.(1) Institutions must establish a risk management function, a compliance function, an information security function and an internal audit function independent from the operational functions and which shall have sufficient authority, stature, resources and access to the management body; subject to approval by the Central Bank, less-complex or smaller institutions may combine the tasks of the compliance function and/or information security function with the tasks of the risk management function.

(2) Internal control functions must have the right on their own initiative to communicate with any staff member and obtain access to any records or files or any other form of information necessary to enable them to carry out their responsibilities.

(3) The internal audit function must report to the management body through the audit committee and inform senior management about its findings, in accordance with the provisions of this Directive.

(4) The risk management function, compliance function and information security function must have the right to report their findings and assessments directly to the management body and the relevant committees, independent from senior management through clear reporting lines.

(5) Internal control functions must ensure that communication with senior management, management body and relevant committees is adequately documented.

Independence of internal control functions.

77.(1) The internal control functions are independent of the business and support units they monitor and control as well as organisationally independent from each other.

(2) A control function is regarded independent if the following conditions are met:

(a) its staff does not perform any tasks that fall within the scope of the activities it is intended to monitor and control and potential conflicts of responsibilities do not arise;

(b) is organisationally separate from the activities it has been assigned to monitor and control;

(c) the remuneration of the internal control function's staff are not -

(i) linked to the performance of the activities it monitors and controls;

(ii) structured in a manner that could compromise the objectivity of their staff.

Head of internal control function.

78.(1) Institutions must ensure that the head of a control function is an independent senior manager with distinct responsibility for the said control function.

(2) The head of an internal control function shall not be removed without prior approval of the management body in its supervisory function and shall be able to have direct access to

the management body where necessary.

(3) The head of an internal control function should demonstrate appropriate leadership and 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 in accordance with this Part;

(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 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) preparing and delivering to newly appointed members of the management body, in coordination with the secretary of the management body, an induction seminar adequately covering the respective areas of responsibilities of the function with references to the responsibilities of the management body and the requirements of the regulatory framework;

(h) in case where the institution is a parent undertaking of a group, expressing an opinion 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 Central Bank of any significant findings on, or developments that came to his/her attention that have material impact on, the 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 Central Bank at least annually or at any other interval the Central Bank may require to discuss the scope and coverage of the work of the internal control function, its risk analysis, findings and recommendations.

Qualification of staff of internal

79.(1) Internal control functions should have an adequate number of qualified staff both at parent and subsidiary level.

control functions.

(2) Staff of internal control functions should be trained on an on-going basis, and should receive proper training.

(3) Institutions shall ensure that staff of internal control functions has appropriate data systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities.

Rotation of internal control functions' staff.

80.(1) Subject to subparagraph (2), institutions should, whenever practicable and without jeopardising the competence and expertise of the internal control functions, periodically rotate staff within an internal control function or from other functional areas of the institution, to ensure that an individual's capacity for critical judgement is not called into question because of possible loss of objectivity from continuously performing similar tasks or routine jobs.

(2) Staff rotations within an internal control function and staff rotations to and from an internal control function should be governed by and conducted in accordance with a sound written policy; this policy must be designed in such a way so as to avoid conflicts of interest and to ensure that:

(a) a cooling period adapted to the size and complexity of the institution elapses before staff rotated to an internal control function from other functional areas of the institution is assigned oversight responsibilities related to the functional area they served before the rotation;

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

Relationship between internal control functions.

81.(1) In view of the close relationship between the activities of the internal control functions, institutions must ensure that there is a clearly identified allocation and division of responsibilities, especially as regards the responsibility for measuring risks as well as identification, verification and assessment of the adequacy of related internal control procedures and regulations.

(2) Internal control functions should communicate to other internal control functions any findings relating to them; such findings should serve as a feedback mechanism to the latter functions in assessing their areas of responsibility in related internal control policies and procedures.

Internal control function charter.

82.(1) The purpose, standing and authority of a internal control function should be governed by a charter which must be periodically reviewed by the head of the internal control function and approved by the management body.

(2) The charter should define, as a minimum, the following:

(a) the internal control function's standing within the institution, its authority, its purpose and scope, its key features and responsibilities, its reporting 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 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.

Internal control function's role in group structures.

83.(1) In case where the institution is a parent undertaking of a group, the institution's internal control function must ensure that the respective internal control functions of subsidiaries report, on a regular basis, on their activities and findings; the institution's internal control function must, based on the activities and findings of the subsidiaries' internal control functions, carry out, on a periodic basis, off-site and on-site reviews of units, branches, subsidiaries in Cyprus and abroad for assessing their compliance with the group's policies and procedures.

(2) In case where the institution is a subsidiary undertaking of a group, the institution's internal control function must report, on a regular basis, to the head of the group internal control function on their activities and findings in areas, functions and activities of the institution.

Subsection 3.1 - Risk management function

General requirements for the risk management

84.(1) The risk management function must ensure that all material risks are identified, measured and properly reported.

(2) The risk management function must be actively involved in elaborating the institution's risk strategy and in all material risk management decisions and it must be able to deliver a

function.

complete view of the whole range of risks of the firm.

(3) Institutions must ensure that the risk management function is able to report directly to the management body in its supervisory function, independent from senior management and that it can raise concerns and warn the management body, where appropriate, where specific risk developments affect or may affect the firm, without prejudice to the responsibilities of the management body in its supervisory and/or managerial functions pursuant to this Directive, the Law and the Regulation (EU) No 575/2013.

Risk management function's role in strategy, risk appetite and decisions.

85.(1) The risk management function must deliver analyses and expert judgement on risk exposures, to enable the management body to set the institution's strategy and risk appetite framework.

(2) The risk management function must assess the risk strategy and risk appetite statement including targets proposed by the business units and advise the management body before a decision is made; targets, which include credit ratings and rates of return on equity, should be plausible and consistent.

(3) The risk management function should be adequately involved in any changes to the institution's strategy, risk appetite framework and risk limits.

(4) The risk management function shall be actively involved at an early stage in the evaluation of the impact of material changes to the institution's structure and exceptional transactions on the institution's and group's overall risk before any decision on such changes is taken.

(5) The risk management function's involvement in decision making processes must ensure that:

(a) its on-going assessment of risk-taking activities must remain objective and independent;
(b) accountability for decisions taken remains with the business and support units and ultimately the management body.

(6) The risk management function should 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.

(7) The requirements set out in this paragraph shall apply to the risk management function of a parent institution regarding the whole group.

Risk management function

86.(1) The risk management function is responsible for the proper planning, development and monitoring of, and reporting on, the risk management framework as provided in Part

’s role in risk manag ement.

IX.

(2) The risk management function must ensure that the risk management framework identifies, consolidates and prioritise the risks faced by the institution.

(3) The risk management function should ensure that the risk identification process of the institution does not focus only on the risks provided in Part IX or financial risks that are easy to measure but examines all dimensions of the risks the institution face including non-financial risks such as legal and reputational risks; risk management function shall be responsible for identifying risks arising from the complexity of the institution’s legal structure and for recognising new or emerging risks arising from changing circumstances and conditions.

(4) The risk management function shall ensure that leading sources of risks identified are recognised in a consistent manner to allow the assessment of interactions between these risks.

(5) The risk management function shall regularly validate the accuracy and effectiveness of the risk management process; such validation exercises shall include at least testing actual outcomes against previous estimates.

(6) The risk management function should independently assess a breach or violation of risk limits, including its cause and a legal and economic analysis of the actual cost of closing, reducing or hedging the exposure against the potential cost of keeping it; the risk management function should inform, as appropriate, the business units concerned and recommend possible remedies.

(12) In case where the institution is a parent undertaking of a group, the risk management function should monitor the risks taken by the subsidiaries and report any inconsistencies with the approved group strategy to the management body.

Risk manag ement function ’s role in develop ing and approvi ng new product s.

87.(1) The risk management function shall actively participate in the process of approving the development in new markets, products and services and significant changes to existing ones, with a clear overview of the roll-out plan across different business lines and portfolios and have the power to require that changes to existing products go through the formal new products approval process in accordance with paragraph 72; Its input should include a full and objective assessment of -

(a) risks arising from new activities under a variety of scenarios;

(b) any potential shortcomings in the institution’s risk management and internal control frameworks; and

(c) the ability of the institution to understand and manage any associated risks.

Specific requirements of the head of the risk management function.

88. The person appointed to carry out the tasks of the head of the risk management function should have sufficient expertise and operating experience enabling the challenging of decisions that affect an institution's exposure to risk.

Risk management function's reporting requirements.

89.(1) The head of the risk management function must submit, on a quarterly basis a report, to the risk committee 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 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 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 institution's operations and risk profile;
(b) description of the risk management framework, including the organization 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 minimizing 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 non-performing loans monitored by the institution;
(h) calculation of the 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 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.

Subsection 3.2 - Compliance function

Compliance function's roles and responsibilities.

90.(1) The compliance function must 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 in accordance with Part VIII 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.

(2) Compliance activities must 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 must 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) ensuring that a fully and updated register of legal, regulatory and business requirements is maintained and that emanating compliance obligations are, documented;

(c) 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;

(d) Identifying and documenting the compliance risks associated with the institution's business activities, on a pro-active basis;

(e) 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;

(f) formulating proposals for organizational and procedural changes to ensure that identified compliance risks are appropriately managed;

(g) 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 in accordance with paragraph 59(4);

  (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;

(h) 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 in accordance with paragraph 57;

(i) overseeing the complaints process and utilizing customer complaints as a source of relevant information in the context of its general monitoring responsibilities;

(j) periodically reassessing and reviewing the scope of compliance reviews to be performed;

(k) cooperating and exchanging information with other internal control and risk management functions on compliance matters;

(l) 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;

(m) organizing regular training and educational programs for management and staff on compliance and regulatory matters;

(n) advising and responding to queries on compliance issues from staff;

(o) 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;

(p) 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;

Compliance function's role on prevention of money laundering activities.

91. The compliance function must ensure the institution's compliance with the Prevention and Suppression of Money Laundering Activities Law of 2007 and subsequent amendments and the CBC Directives and circulars for the prevention of money laundering and terrorist financing issued in accordance with article 59(4) of the said Law; the head of the compliance function or another member of the compliance function holding a managerial position should be appointed to the post of Money Laundering Compliance Officer under section 69 of the said Law.

Compliance function's role in institutions providing investment services and activities.

92. Institutions that provide investment services and activities and ancillary services in accordance with the Investment Services and Activities and Regulated Markets Law of 2007 must ensure that the compliance function is involved in the development of the relevant policies and procedures within the institution; the compliance function should periodically assess the institution's compliance with the provisions of this law including whether staff in the area of investment services and activities holds the necessary level of awareness and correctly apply the institution's policies and procedures.

Compliance function charter.

93. In case where compliance responsibilities are carried out by staff in different responsibilities, the compliance charter should define how these responsibilities are to be allocated among the departments.

Reporting requirements.

94. (1) The head of the compliance function must submit, on a quarterly basis a report, to the audit committee 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 institution;

(b) material compliance issues and the status of any associated investigations or other actions being taken;

(c) updated 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 organization 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 updated 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;

(f) details on the above for each subsidiary in Cyprus and abroad and foreign branches;

(h) an update summary of material correspondence with competent authorities;

(i) the compliance programme and action plan of the compliance function for the following year.

Subsection 3.4 – Information security function

Information security function's roles and responsibilities.

95. (1) The information security function shall be responsible and accountable for the development and implementation of the information security framework; as a minimum it must -

(a) advise and provide recommendations to management body on the development of an information security policy in line with the institution's size and complexity of activities and information distribution channels;

(b) advise and provide recommendations to senior management on the development and implementation of the institution's information security program in the form of security policies, standards, guidelines, procedures and processes; it must ensure that, inter alia, the following are developed, documented and implemented:

(i) information classification policies and standards designed to provide information owners with guidance on how to classify information assets properly and how to determine the appropriate level of protection and procedures for the appropriate disclosure, modification, removal, or destruction of information assets;

(ii) policies and procedures to ensure that information systems acquired, developed and maintained adhere to the institution's information security policy;

(iii) policies and procedures for the management of access rights to the institution's information systems;

(iv) security incident response, tracking and escalation procedures and a formal procedure for developing, documenting and implementing corrective action plans to avoid recurrence;

(v) appropriate controls in existing and new operating procedures, including the appropriate segregation of duties;

(vi) procedures for the protection of the institution's information during the course and upon cessation of contracts with vendors and third parties and termination of employment, long term leave of absence, transfer, or change of duties;

(vii) policies and procedures designed to prevent unauthorized physical access to the institution's information assets and damage from man-made or natural disasters.

(c) oversee the dissemination and implementation of the information security program institution-wide;

(d) cooperate with the institution's business and support units and other internal control functions, for the effective implementation of security principles in the development of their policies and procedures; interaction between business and support units

and other internal control functions and the information security function should facilitate the objective that all the institution's staff bears responsibility for protecting the institution's confidential and proprietary information;

(e) develop and implement, in cooperation with the risk management function, an information security risk assessment and management program;

(f) participate in the activities required for the implementation of effective security controls in the institution's information technology infrastructure and provide guiding principles to the information technology unit responsible for the operation of the institution's network and information systems;

(g) plan, organise and coordinate information security assessment activities throughout the institution;

(h) monitor compliance with information security policies, standards, guidelines, processes, and procedures.

(2) The information security function must be actively involved in the development and implementation of an education and training program on information security and privacy matters for all employees of the institution, including senior management.

Reporting requirements.

96. The head of the information security 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; the report should cover, as a minimum, the following:

(a) a summary of the most important information security risks the institution faces at the time of reporting;

(b) a list of all important information security incidents which took place during the year and corrective actions taken to prevent recurrence;

(c) any important actions taken in the year preceding the report to improve weaknesses in the information security environment; and

(d) any outstanding issues which jeopardize the institution's information security.

Subsection 3.5 – Internal audit function

Role and responsibilities of internal audit function.

97. (1) The internal audit function must be able to perform audit assignments in accordance with paragraph 0 on its own initiative in all areas and functions of the institution including the institution's outsourced activities, according to the audit plan prepared by the head of the internal audit function and approved by management body in accordance with paragraph 101 to provide independent assurance to the management body in respect of matters such as:

(a) the appropriateness, adequacy and effectiveness of the governance framework;

(b) the overall means by which the institution manages and mitigates risks to preserve its assets, and seeks to prevent fraud, misappropriation, or misapplication of such assets;

(c) the reliability, integrity, and completeness of the accounting, financial reporting, and management information and information technology systems;

(d) the design and operational effectiveness of the institution's individual controls and internal control functions in respect of the above matters, as well as of the totality of such controls;

(e) other matters as may be requested by the management body, senior management or the Central Bank; and

(f) other matters which the internal audit function determines require review to fulfil its mission, in accordance with the internal audit charter.

(2) The internal audit function should not be involved in designing, selecting, implementing or operating specific internal control measures; internal audit function may provide input on matters related to risks and internal controls upon request by the senior management for as long as the independence of audit assignments is not called into question.

Internal audit charter.

98. (1) In addition to the provisions of paragraph 82 , the internal audit charter should empower the internal audit function, whenever relevant to the performance of its assignments, to initiate direct communication with any member of staff, to examine any activity or entity of the institution including other internal control functions, and to have full and unconditional access to any records, files, data and physical properties of the institution including access to management information systems and records and the minutes of all consultative and decision-making bodies.

(2) The internal audit charter should also define procedures for the coordination of the internal audit function with the external auditors.

Audit assignments.

99. (1) The internal audit function must carry out such assignments as are needed to fulfil its responsibilities to provide assurance in accordance with paragraph 0, through routine audits and special audits, both announced and unannounced.

(2) The following audit activities should 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 institution has established appropriate corporate governance policies and procedures;

(b) assessment of the extent to which the institution's collective bodies as well as its operational units and internal control units effectively utilize 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 in line with the principles mentioned in Appendix 3;

(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 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) the evaluation on the completeness and effectiveness of the outsourcing policy;

(i) the assessment of the completeness and adequacy of the institution's Business Continuity and the Information Technology Disaster Recovery Plans;

(j) the assessment of the completeness and adequacy of the institution's information security policy, including Information Technology security;

(k) the evaluation of the process for assessing the institution's capital adequacy relative to its risk profile (ICAAP), the parameters upon which the institution has based its capital adequacy calculations and the review of the process for stress testing the 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 information security function.

Audit plan.

100. (1) The audit plan should be risk-based and dynamic, aiming to ensure all entities and all activities of the institution are audited at least once within an appropriate period of time. The audit plan should be a means of assessing the adequacy and effectiveness of the internal control framework.

(2) The audit plan should 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 loan origination;

(ii) the correct application of the internal credit rating system developed by the 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 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:

(i) the risk management framework;

(ii) the information systems; and

(iii) 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 annual basis in accordance with the provisions of the aforementioned Directive;

(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 must 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;

(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 to management body.

101. (1) The head of the internal audit function shall report to the management body through the audit committee, at least on a quarterly basis, of all major observations 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;

(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 Central Bank, especially COREP, FINREP, large exposures, prudential liquidity and facilities to members of the management body, major shareholders and their connected persons;

(e) the audit and action plan for the following year.

Internal audit function's interaction with the Central Bank.

102. The head of the internal audit function's interaction with the Central Bank should cover the following topics for the purposes of paragraph 78(3)(i)-(k), based on the results of the assessments carried out:

(a) the adequacy and effectiveness of the institution's processes for objective setting and strategic decision making;

(b) the quality and substance of management and governance structure and processes;

(c) the 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 63 to71;

(d) the institution's business model including risks in the institution's business activities, processes and functions and the adequacy of the control and oversight of these risks such as:

  (i) application and effectiveness of risk management procedures and risk assessment methodologies as applied to material risks including the risks referred to in paragraphs 63 to71;

  (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) significant transactions;

  (v) handling of non-performing and problematic loans;

  (vi) frauds;

  (vii) outsourcing arrangements;

(e) issues related to business conduct such as:

  (i) management of conflict of interest;

  (ii) adherence to rules for providing services to clients;

  (iii) anti-money laundering processes and controls;

(f) issues related to internal controls and adequacy and effectiveness of other internal control functions.

Qualifications and skills and professional care of internal audit staff.

103. (1) A person appointed as internal auditor must possess the necessary professional competence and due professional care for the effective discharge of his or her duties.

(2) An internal auditor must, as a minimum, have the knowledge, experience and capacity in -

(a) applying suitable audit methodologies, tools and techniques for-

(i) the collection and processing of information; and

(ii) the examination and evaluation of audit evidence; and

(b) communicating in a clear and effective manner with the stakeholders of the internal audit function.

(3) An internal auditor must -

(a) act with integrity, carrying out his or her duties in an honest and professional manner and informing the head of internal unit function if his or her fitness to carry out an audit assignment is called into question;

(b) be diligent in the protection of information acquired in the course of his or her duties;

(c) ensure that his or her professional judgment is not influenced by any personal or commercial consideration; internal auditors recruited internally should not engage in auditing activities for which they have had previous responsibility before a sufficiently long cooling off period has elapsed.

Subsection 4 – External assessment of the adequacy of the internal control framework

External assessment of the internal control framework.

104. (1) Institutions should 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 institution's statutory external auditor, who possess the necessary expertise in carrying out the required assessment in accordance with the provisions of Appendix 1.

(2) The assessment referred to in subparagraph (1) should be conducted on a consolidated basis as well as on an individual company basis.

(3) Institutions should rotate external auditors referred to in subparagraph (1) after two consecutive assessments.

PART XI
INFORMATION SYSTEMS AND BUSINESS CONTINUITY

Information systems.

105. (1) Institutions must have in place effective and reliable information and communication systems covering all of their significant activities.

(2) Institutions must ensure that the information systems generate timely, accurate, consistent, complete and relevant information to enable -

(a) the compilation of annual or periodic financial or non-financial statements on the institution's financial and risk profile, for internal or external purposes;

(b) effective management decision making and oversight;

(c) informed judgements about the effectiveness of -

(i) the management body, senior management and internal control functions;

(ii) the risk management framework, compliance framework and internal control framework.

(3) Information systems including those that hold and use data in electronic form, should be secured, independently monitored and supported by adequate contingency arrangements; institutions must implement the framework of principles for the secured and effective operation of information and technology systems outlined in Appendix 3.

(4) Institutions must ensure that records on transactions are maintained in a systematic and secured manner for a time period not less than ten (10) years and in a manner which facilitates an audit trail and reconstruction of all transactions in a chronological order, the verification of each recorded transaction against original vouchers and the validation of any changes in the balances of accounts with supporting data covering all transactions leading to the above changes.

Contingency and business continuity plans.

106. (1) Institutions must have in place adequate contingency and business continuity plans aimed at ensuring that, in the case of a severe business disruption, they will be able to operate on an ongoing basis and that any losses will be limited; the contingency and business continuity plans should be implemented as per the framework of principles for the sound and effective operation of information technology systems, which is outlined in Appendix 3.

(2) Institutions must ensure that internal control functions are actively involved in the establishment, monitoring and oversight of the contingency and business continuity plans.

PART XII
TRANSPARENCY

Empowerment of staff.

107. Institutions must ensure that strategies and policies are communicated to all relevant staff throughout an institution in a clear and consistent way, at least to the level needed to carry out their particular duties, through written guidelines, manuals or other means.

Public disclosures.

108. (1) Institutions must ensure that appropriate and adequate policies, processes and

systems are in place for the timely, and accurate public disclosure of information to stakeholders on their current position and future prospects.

(2) Any information publicly disclosed about the current financial position of institutions should comply with any legal, regulatory or listing disclosure requirements and should be clear, accurate, relevant, timely and accessible.

(3) Institutions are required to disclose on their website and promptly update the following information on their corporate structure and internal governance in a clear and visible manner:

(a) ownership structure, qualifying shareholders, share ownership and voting rights, beneficial owners of qualifying shareholders in case of legal persons, participation of qualifying shareholders on the management body or in senior management positions, core business;

(b) when an institution operates in jurisdictions that impede transparency or through complex structures, information regarding the purpose, strategies, structures, risks and controls of such operations;

(c) governance structures and policies, including its objectives, organisational structure, internal governance arrangements, reporting lines;

(d) management body's structure, bylaws, composition, selection process, member qualifications, directorships of members in other organisations, attendances to meetings, independence criteria, committees' membership composition, responsibilities and terms of reference of committees;

(e) senior management's structure, its responsibilities, qualifications and experience;

(f) information regarding the institution's incentive scheme, remuneration policies, salaries, executive compensation, bonuses, stock options;

(g) the code of business conduct and corporate values and the process by which they are implemented in the organisation;

(h) the nature, extent, purpose and economic substance of material transactions with members of the management body and connected parties; these transactions must be published within five (5) working days;

(i) a description of the internal control framework, the manner internal control functions are organised, the major tasks they perform;

(j) where an institution is state-owned, the overall objectives of state ownership, including any special obligations of the institution with regards to the social policy of the state, how these obligations are financed as well as the policy and role of the state in the institution's internal governance.

(4) Institutions must explain in their website how they comply with the requirements of

paragraphs 5, 6(a), 7(3)-(4), 9, 15(2), 20(1)-(2), 22(1)-(2), 23(3), 24(1), 25(1)(c), 25(5), 34(2), 35, 43, 44 and 49 to 52 and Appendix III of the Fitness and Probity Directive of 2014.

(5) In cases where ensuring a high degree of accuracy would delay the release of time-sensitive information, should make a judgement as to the appropriate balance between timeliness and accuracy, bearing in mind the requirement to provide a true and fair picture of its situation and give a satisfactory explanation for any delay; this explanation should not be used to delay regular reporting requirements.

PART XIII
REPORTING TO THE CENTRAL BANK

Reporting to the Central Bank.

109. (1) Institutions must submit to the Central Bank the finalised minutes of the meetings of the audit committee and risk committee as provided in paragraph 7(4) within one (1) month from the meeting date

(2) Institutions must submit to the Central Bank within three (3) months of the end of every year, the following reports and information, together with the corresponding assessments of the competent committees of the management body and the relevant extracts from the minutes of the management body's meetings:

(a) annual report on the internal control framework prepared by the head of the internal audit function;

(b) annual report on the management of risks, prepared by the head of the risk management function;

(c) annual report on compliance, prepared by the head of the compliance function;

(d) annual report on information security, prepared by the head of the information security function;

(e) evaluation report on the performance of the management body as whole, its committees and individual members prepared by the management body in accordance with paragraph10 including the appraisal of the chairperson of the management body;

(3) Institutions must submit to the Central Bank the semi-annual report of the outsourcing officer provided in Appendix 2 within one (1) month from the end of the period covered.

(4) Institutions must submit to the Central Bank annually by 30 June each year –

(a) the information disclosed in accordance with the criteria for disclosure established in points (g), (h) and (i) of Article 450(1) of Regulation (EU) No 575/2013; for the purposes of this point, institutions must complete and submit the templates

provided in Annexes 1-3 of the EBA guidelines on the remuneration benchmarking exercise of 2014 as amended or replaced in accordance with the requirements set out in Titles III and IV of the said EBA guidelines;

(b) information on the number of natural persons per institution that are remunerated EUR 1 million or more per financial year, in pay brackets of EUR 1 million, including their job responsibilities, the business area involved and the main elements of salary, bonus, long-term award and pension contribution; for the purposes of this point, institutions must complete and submit the templates provided in Annex 1 of the EBA guidelines on the data collection exercise regarding high earners of 2014 as amended or replaced, in accordance with the requirements set out in Titles II and III of the said EBA guidelines;

(c) the policy on diversity with regard to selection of members of the management body as provided in paragraph 9(1) and disclosed in accordance with the Article 435(2)(c) of Regulation (EU) No 575/2013.

(5) Institutions must submit to the Central Bank the assessment reports on the adequacy and effectiveness of the internal control framework on a solo and consolidated basis prepared by external auditors in accordance with paragraph104.

(6) Institutions must submit to the Central Bank the assessment reports on the composition and operations of the management body and its committees prepared by an external consultant in accordance with paragraph 10; the next report must be prepared and submitted to the Central Bank by 31 December 2014 and the reports to follow should be submitted with the reports submitted in accordance with subparagraph (1).

PART XIV
MISCELLANEOUS

Date of entry into force.

110. The provisions of this Directive enter into immediate effect.

Extension of period for compliance with this Directive.

111. Institutions shall within one (1) month from the date of entry into force of this Directive inform the Central Bank if they do not comply with the provisions of paragraphs 6(a), 9(3)-(4), 35(2) and 76(1) and provide the Central Bank with a timetable for rectifying their position which shall not exceed one (1) year from the date of entry into force of this Directive;

Compliance with remuneration principl

112. Institutions are required to apply the principles laid down in Part VI to remuneration awarded for services provided or performance from the year 2014 onwards, whether due on the basis of contracts concluded before or after the date of entry of this Directive.

es.

Repeal. 113. The Directive issued by the Central Bank to banks on the framework of principles of operation and criteria of assessment of banks' organisational structure, internal governance and internal control systems of 2006 to 2012, is hereby repealed.

APPENDIX 1

(Paragraph 0)

CONTENTS OF THE REPORT ON

THE ASSESSMENT OF THE ADEQUACY OF THE INTERNAL CONTROL FRAMEWORK

PREPARED BY EXTERNAL AUDITORS

PART I

INTRODUCTION

1. (1) The assessment must be carried out in accordance with best international practices in order to ensure that the internal control system meet the standards required in this Directive.

(2) The assessment on the adequacy of the internal control framework must 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 institution's key departments / divisions / units, their terms of reference, procedures and information technology used.

2. Prior to the commencement of the work, the audit committee of the institution must specify the units and subsidiaries to be included in the scope of the assessment. This will be based on the principle of proportionality as well as on other qualitative criteria. The scope of assessment must be submitted in advance to the Central Bank.

3. Upon completion of the assessment, the external auditors must issue a report on their opinion in relation to 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 must be reviewed by the institution's audit committee.

PART II

MINIMUM ASPECTS OF ASSESSMENT

4. The report must cover, as a minimum, assessment / examination of the following:

(a) Organisation structure

(i) The organisational structure (organisational chart and reporting lines, composition, terms of reference and functioning of the management body and its committees);

(ii) The general framework for corporate governance to assess as to whether it is in accordance with the provisions of the Directive and ensures prompt and precise communication of all material issues relating to the 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 framework;

(v) Conflict of interest, four eyes principle and segregation of duties; and

(vi) The procedure for the preparation of the annual budget in line with the 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 must be assessed. The assessment should 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;

(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) 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. In relation to the internal audit function, its independence, position on the organisational chart and its connection to the management body and audit committee should be examined;

(ii) practices and internal audit methodology which must be compared with best practices;

(iii) 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 institution;

(iv) on a sample basis, the adequacy of audit reports for the institution and its subsidiaries prepared by the internal audit function;

(v) the monitoring procedure for the compliance of audited units with the recommendations of the head of the internal audit function; and

(vi) external quality assessment review of the internal audit function.

(e) Risk committee and risk management function

(i) The composition and role of the risk committee;

(ii) the 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 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 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 institution; and

(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 institution and for securing their non-preferential treatment.

(f) Compliance function

(i) 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) The 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) Information Security Function

(i) The information security 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) The 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) The adequacy of the policies and procedures in place for effective information security management as well as effective information security risk treatment in the institution;

(iv) The existence of adequate monitoring and reviewing processes for the purpose of continuing information security improvement in the institution.

5. The assessment of the internal control system of the holding institution and its subsidiaries must be conducted in the same way.

APPENDIX 2
(Paragraph 21)
OUTSOURCING
PART I

INTRODUCTION AND DEFINITIONS

1. For the purposes of this Appendix:

«Outsourcing Service Provider» means the supplier of a service or activity, which may be a separate legal entity within the group or an entity that is external to the group;

«Critical or important service or activity» means the service or activity whose possible improper or inappropriate or failure to execute, would materially impair the ongoing compliance of the institution with the terms and conditions under its license, or the ability of the institution to meet its regulatory responsibilities or it would affect its financial results, its soundness or the continuity of the business of the institution;

The following services or activities are considered to be critical or important, however these cases should not be considered as exhaustive:

(i) functions which are integral or closely related to the business of a Credit Institution, as defined in sections 3 and 13(3) of the Law;
(ii) the internal control functions
(iii) the administration of institution's core banking systems and any other systems being the source of information for financial and regulatory reporting;
(iv) the administration of the institution's information and communication technology infrastructure.

Critical or important services or activities

2. Outsourcing of services or activities that are considered to be critical or important, including intra-group outsourcing of critical or important services or activities, is not allowed without the prior written approval of the Central Bank. The application submitted to the Central Bank of Cyprus requesting approval for outsourcing of services or activities that are considered to be critical or important should contain, at least of, the following information:

(a) the owner department / unit of the institution;
(b) a description of the outsourced service or activity;
(c) details of the outsourcing service provider. In the case the outsourcing service provider is under the supervision of another competent supervisory authority, details of the other competent authority should be provided.
(d) a confirmation that the outsourcing process is in compliance with the provisions of this Appendix, including a confirmation that a risk assessment has been carried out by the Risk Management Function and that legal advice has been obtained;

(e) a confirmation that a formal approval for outsourcing has been obtained at the appropriate hierarchical level;
(f) a confirmation that, subject to Central Bank approval, a formal outsourcing agreement between the institution and the service provider will be prepared and signed, in full compliance with the provisions of this Appendix.

Services or activities which are not considered to be critical or important

3. In the case of outsourcing of services or activities which are not considered critical or important, institutions are required to inform in writing the Central Bank by submitting a report on a six-monthly basis stating all the outsourced services or activities which are not considered critical or important. The said report should be submitted by the Outsourcing Officer no later than 31 July for the first six months of the year and by 31 January for the remaining six months of the year in question. The report should, inter alia, include the following:

(a) the owner department / unit of the institution;
(b) a brief description of the service or activity;
(c) details of the outsourcing service provider;
(d) Initial date of the outsourcing agreement and duration;
(e) a confirmation that the outsourced service or activity is not considered critical or important, and that to this end a formal legal opinion has been obtained;
(f) a confirmation that an appropriate risk assessment has been carried out based on the materiality of the outsourced service or activity; and
(g) a confirmation that a formal approval for outsourcing has been obtained at the appropriate hierarchical level.

PART II
RESPONSIBILITIES OF THE OUTSOURCING OFFICER

4. Institutions are required to appoint an Outsourcing Officer for liaising with the Central Bank of Cyprus on outsourcing issues. However, it is required that within the institution, the competent departments and/ or units bear full responsibility for outsourcing and compliance.

5. The Outsourcing Officer, inter alia, is responsible for:

(a) ensuring that the outsourcing process is conducted by each department/unit according to the institution's policy and procedures and in line with the requirements of this Appendix;
(b) ensuring that a legal opinion is obtained as to whether an outsourced activity is considered to be or not critical/important;
(c) ensuring that a comprehensive outsourcing risk management procedure is established by the

Risk Management ~~Unit~~ Function, where necessary;

(d) ensuring that a risk assessment has been appropriately carried out for each activity to be outsourced;

(e) acting as a central point for liaising with the Central Bank of Cyprus for outsourcing issues and provides all necessary information requested by the Central Bank of Cyprus;

(f) maintaining a comprehensive and updated inventory of all outsourced services or activities;

(g) preparing an annual report which shall include the services or activities outsourced during the year with special emphasis to the outsourced activities or services that are considered to be critical or important. The report should be submitted to the senior management.

PART III
BASIC PRINCIPLES OF OUTSOURCING

6. In the course of its decision making process for outsourcing, an institution should be guided by and apply the following basic principles:

(1) The institution should ensure that an appropriate risk assessment has been conducted for each outsourcing.

In the case of outsourcing services or activities which are considered critical or important or any other service or activity that an institution may decide, a risk assessment must be conducted from the risk management function of the institution.

In the case of outsourcing services or activities which are not considered critical or important, an appropriate risk assessment should be conducted, based on the materiality of the outsourced service or activity.

(2) When establishing a risk assessment, it should take into consideration a number of factors, such as the scope of the outsourced service or activity, the ability of the institution to identify, monitor, manage and control outsourcing risks and the ability of the outsourcing service provider to manage and control the potential risks of the operation. The following factors should also be considered:

(a) the financial, operational and reputational impact on the institution resulting from the failure of an outsourcing service provider to adequately perform the service or activity;

(b) the cost;

(c) potential losses to the institution's customers and their counterparts in the event of a outsourcing service provider failure;

(d) consequences of outsourcing the service or activity on the ability and capacity of the institution to conform with supervisory / regulatory requirements as well as respond to changes in the supervisory / regulatory requirements;

(e) interrelationships and interdependencies of the outsourced service or activity with other services or activities within the institution;
(f) affiliation or other relationship between the institution and the outsourcing service provider;
(g) the fitness and probity of the outsourcing service provider, as well as whether he is subject to any regulation and supervision;
(h) the degree of difficulty and time required to select an alternative outsourcing service provider or to bring the business service or activity in-house, if necessary;
(i) the complexity of the outsourcing arrangement. For example, the ability to control the risks where more than one outsourcing service providers collaborate to deliver an end-to-end outsourcing solution;
(j) the risk concentrations, risks arising from outsourcing multiple services or activities to the same outsourcing service provider;
(k) the limits on the acceptable overall level of outsourced services or activities; and
(l) the possibility to insure, wholly or partly, the risks undertaken.

In addition to the above, an institution should also consider the data protection and security as well as other risks which may be negatively impacted by the geographical location of the outsourcing service provider. Specific risk management expertise in assessing country risk (i.e. risks related to political, financial or legal conditions) could, therefore, be required when entering into and managing outsourcing arrangements with outsourcing service providers located outside Cyprus.

In general, a comprehensive risk assessment should provide for a continuous monitoring and controlling of all relevant aspects of the outsourcing arrangements, including guidance for corrective actions to be taken when certain events occur.

(3) The institution should ensure that the outsourcing arrangements do not diminish the ability of the institution to fulfil its obligations towards customers and therefore should not affect the rights of a customer against the institution, including the ability of the customer to obtain compensation.

(4) The institution should ensure that the outsourcing service provider complies with its legal and regulatory requirements.

(5) The institution should ensure that outsourcing arrangements should not impair the ability of the Central Bank to exercise its regulatory authorities such as proper supervision and regulation of the institution. A service or an activity should not be outsourced if this would impair the right of the Central Bank to assess or its ability to effectively supervise the business of the institution.

(6) The institution should exercise appropriate due diligence when selecting outsourcing service providers. Institutions should develop criteria which will enable them to assess, prior to selection, the outsourcing service provider’s capacity and ability to perform the outsourced services or activities effectively, reliably and to a high standard, together with any potential risk factors

associated with using a particular outsourcing service provider. Services or activities should not be outsourced to a service provider that does not meet the institution's criteria. Appropriate due diligence should include:

(a) The identification of any conflicts of interest or potential conflicts of interest due to the fact that the outsourcing service provider constitute a group of connected persons with:
  (i) any member of the institution's or the group's senior management or management body;
  (ii) the institution's external auditors or
  (iii) the institutions external legal advisors;
(b) the selection of outsourcing service providers which are qualified and which possess adequate resources to perform the outsourcing work;
(c) ensuring that the outsourcing service provider understands and can meet the objectives of the institution in the specified service or activity;
(d) recognition of the outsourcing service provider's financial soundness to fulfill its obligations. Any special needs, such as servicing geographically dispersed services or activities, must be determined and met by using third parties with similar reach and capability;
(e) areas of concern:
  (i) If an outsourcing service provider fails or is, otherwise, unable to perform the outsourced service or activity, it may be costly and / or problematic to find, timely, alternative solutions;
  (ii) transition costs, potential business disruptions and potential business loss of existing or new businesses should also be considered; and
  (iii) additional concerns exist when outsourcing a service or an activity abroad. For example, in an emergency, an institution may find it more difficult to respond on time. In this regard, the Senior Management of the institution may need to assess the economic, legal and political conditions that might have a negative impact on the outsourcing service provider's ability to perform effectively for the institution.

(7) In general, the Central Bank of Cyprus requires that institutions ensure that they remain in charge of their own business, in control of their existing business risks as well as of the new risks introduced by outsourcing and, finally, that they fully comply with their regulatory responsibilities and their responsibilities to their customers.

Contracts and service level agreements

7. The institution should ensure that outsourcing relationships are governed by written contracts and service level agreements that clearly and in detail describe all aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties. The nature and details of such contracts should be appropriate to the materiality of the outsourced service or

activity in relation to the ongoing business of an institution. Appropriate contractual provisions can reduce the risk of non-performance or disagreements regarding the scope, nature and quality of the service to be provided. Some key provisions of such a contract are the following:

(a) the contract should clearly define which services or activities are going to be outsourced, including appropriate service and performance levels. The outsourcing service provider's ability to meet performance requirements, in both quantitative and qualitative terms, as well as his ability and willingness to comply with the requirements of this appendix should be assessed in advance;

(b) the contract should clearly define and specify the respective rights and obligations of the institution and the outsourcing service provider;

(c) the contract should not prevent or impede an institution from meeting its respective supervisory / regulatory obligations or the Central Bank from exercising its supervisory / regulatory powers;

(d) the contract should explicitly provide that the Central Bank of Cyprus has the right, at any time deemed appropriate to:

  (i) Have access to all books, records, information, persons and facilities of the outsourcing service provider, relevant to the outsourced service or activity;

  (ii) request directly from the outsourcing service provider any information in the form of ad hoc or periodic reports;

  (iii) contact directly the outsourcing service provider for the purpose of carrying out on site audits, proportionate to the audit which it would carry out if the institution was performing the outsourced service or activity itself.

(e) the contract should explicitly provide that the institution has the ability to access all books, records, information, members of the staff and facilities relevant to the outsourced service or activity;

(f) a contract should provide for the continuous monitoring and assessment by the institution of the outsourcing service provider so that any necessary corrective measures can be taken promptly;

(g) a contract should describe clearly and in detail all aspects of the exit policy, upon normal or abnormal contract termination. A termination clause and minimum periods to execute a termination provision should be included. The above would allow the outsourced services to be transferred to another outsourcing service provider or to be incorporated back into the institution. Such a clause should include provisions relating to insolvency or other material changes in the corporate form of the outsourcing service provider as well as a clear definition of the ownership of any intellectual property following termination, including transfer of information, data and / or all forms of know-how back to the institution;

(h) material issues unique to the outsourcing arrangement should be addressed. For example,

where the outsourcing service provider is located abroad, the contract should include choice-of-law provisions. Also mechanisms should be in place in order to provide for the resolution and settlement of disputes between the parties under the applicable laws;

(i) a contract should include, where appropriate, conditions of subcontracting by the outsourcing service provider for all or part of an outsourced service or activity. In cases where appropriate, the outsourcing service provider should seek the approval of the institution, prior to assigning to subcontractors all or part of the service or activity. Furthermore, in cases of subcontracting significant part of a service or activity that is considered to be critical or important, then the prior approval of the Central Bank of Cyprus is required. In general, the contract should provide the institution with the ability to maintain a similar control over the risks when the outsourcing service provider outsources to other third parties as in the original direct outsourcing arrangement. It is understood that the third party provider should fully comply with the obligations existing between the institution and the outsourcing service provider;

(j) a contract should include an obligation on the outsourcing service provider to immediately inform the institution or the Central Bank directly of any material changes in circumstances which could have a material impact on the continuing provision of services;

(k) a contract should include a confidentiality clause; and

(l) in preparing, negotiating, renewing or amending an outsourcing contract, an institution should seek legal advice.

Business continuity and disaster recovery

8. The institution should ensure that, in the case of outsourcing services or activities which are considered critical or important or any other services or activities that an institution may decide, the outsourcing service providers establish and maintain contingency plans, including a disaster recovery plan and periodically test these plans adequately. The said plans should comply with the regulatory requirements of the institution and they should be tested and be fully operational prior to the commencement of the outsourced services or activities. More specifically,

(a) an institution should take appropriate steps to assess and address the potential consequence of a business disruption or other problem at the outsourcing service provider. It should request the preparation of appropriate contingency plans by the outsourcing service provider and the co-ordination of the contingency plans at both the institution and the outsourcing service provider;

(b) an institution should also have contingency plans in the event of non-performance by the outsourcing service provider. The contingency plans, must account for the costs of alternative options, in case of deteriorating performance;

Information security and data protection

9. (1) The institution should ensure that appropriate steps are taken to ensure that outsourcing service providers utilize at least an equal level of information security, as required by Appendix 3, for the protection of the institution's proprietary and confidential information, including customer information. Such steps may include provisions in the contract prohibiting the outsourcing service provider and its subcontractors from using or disclosing the institution's proprietary information or that of its customers, except where necessary to provide the contracted services and to meet regulatory and statutory provisions.

(2) An institution should consider whether it is appropriate to notify customers that customer data may be transmitted to an outsourcing service provider, taking into account any regulatory or statutory provisions that may be applicable.

PART IV
RESPONSIBILITIES OF THE MANAGEMENT BODY

10. The management body retains the overall responsibility of outsourced services or activities including the following:

(a) setting, approving and regularly reviewing the institution's outsourcing policy. The outsourcing policy should cover all aspects of outsourcing, including non critical or important outsourcing and whether the outsourcing takes place within the group or not. The outsourcing policy should guide the assessment of whether and how services or activities can be appropriately outsourced to an outsourcing service provider and it should, inter alia, include the following:

(i) a clear definition of the services or activities that may be outsourced as well as the needs and the objectives to be served by the outsourcing solutions;

(ii) provisions ensuring that prior to any outsourcing, the institution develops a comprehensive understanding of the associated benefits, costs and risks involved. This requires an analysis and an assessment of the institution's core activities, its strengths, weaknesses as well as future plans and goals prior to any such outsourcing.

(iii) provisions ensuring that the outsourced services or activities must continue to meet the performance and quality standards that would apply if the institution was to perform these services or activities in-house;

(iv) provisions for any intra-group outsourcing (e.g. to a separate legal entity within the group);

(v) provisions to ensure the ability of the institution to comply with its legal and regulatory requirements;

(vi) provisions to ensure that a service or an activity should not be outsourced if this would impair the right of the Central Bank to assess or its ability to supervise the business of the institution;

(vii) provisions to ensure that an institution has in place procedures to oversee effectively the service or activity being outsourced;

(b) overseeing and assessing the effectiveness of implementation of the outsourcing policy and ensuring its improvement.

PART V

RESPONSIBILITIES OF THE SENIOR MANAGEMENT

11. The Senior Management is responsible for:

(a) Implementing the outsourcing policy as approved by the management body and establishing the procedures to be followed when outsourcing a service or activity;

(b) establishing the procedures for selecting the outsourcing service provider in line with the requirements of this Directive;

(c) defining the main provisions that should be included in the outsourcing agreement, in line with the requirements of this Directive;

(d) evaluating the completeness and effectiveness of implementation of the outsourcing policy and procedures and determining ways for addressing any issues raised and improvement, based on an annual report submitted by the Outsourcing Officer as well as the observations of the Internal Audit submitted to the Audit Committee;

(e) appointing a manager or a person who has the expertise and authority to deal with this issue of the institution as an Outsourcing Officer and communicating to the Central Bank of Cyprus the name, position and contact details of the Outsourcing Officer when the latter is appointed or replaced.

APPENDIX 3

(Paragraph 105)

PRINCIPLES FOR A SOUND AND AN EFFECTIVE OPERATION OF INFORMATION TECHNOLOGY SYSTEMS IN THE CONTEXT OF MANAGING OPERATIONAL RISK

PART I

INTRODUCTION

1. (1) This Appendix outlines a framework of general principles and criteria for the sound and effective operation of Information Technology Systems taking into consideration, at the same time, the most recent developments in information technology to the extent to which they affect the operations of institutions.

(2) This framework constitutes a basis for the evaluation of institutions in this particular sector and the application of its principles is expected to contribute considerably towards the effective management of the operational risk related to Information Technology Systems.

(3) The above principles are grouped into the following four categories:

(a) organisation and governance of information technology, addressing issues of information technology management, the organization of the Information Technology Unit and the relationships with external third parties.

(b) development and commissioning of systems, addressing the issues of methodologies, standards, and procedures for the development and commissioning of Information Technology Systems.

(c) operations and support, addressing the procedural aspect of operating the systems, the systems' security at the physical and logical levels as well as issues related to ensuring the business continuity of a institution.

(d) control of the information technology systems, addressing basic issues and requirements for the sufficient and effective operation of the Internal Audit Unit with regard to Information Technology Systems.

PART II

ORGANISATION AND GOVERNANCE OF INFORMATION TECHNOLOGY

Governance of information technology

2. (1) Information technology governance is the responsibility of the senior management of an institution. It includes a set of appropriate operational structures and processes via which it is ensured that information technology supports the strategy and the objectives of the institution, manages effectively the resources made available to it, evaluates and manages effectively the risks emanating from operating the Information Technology Systems, strictly applies the information security policy, ensures that it can measure its effectiveness and efficiency and, finally, it implements a set of controlling mechanisms in the context of the overall general control framework.

(2) In order to achieve all the above, institutions:

(a) must have a documented and formally approved by the management body strategy on information technology, compatible with their general operational strategies. A thorough and precise strategic plan should exist for the short-term (annually) and a target strategic plan should exist for the medium-term (three years). The institution should also have a strategic view towards its long-term (five years and above) IT landscape. The information technology strategy should achieve the operational objectives set by the senior management of the institution as well as develop, in time, the necessary technological infrastructure for the future needs of the institution.

(b) should establish a specialized IT Steering Committee. To this extent, it is recommended that the Chairperson of this Committee is a member of the institution's senior management with adequate knowledge on information technology issues. The Committee's members should comprise senior management and relevant control functions. The role, the duties as well as its minimum composition should be defined in its official terms of reference. As a minimum, the committee should determine prioritisation of IT investment and projects, in line with the institution's strategic goals, and track status of projects and resolve conflicts. This Committee should receive a copy of all reports prepared and conclusions drawn after all audits and controls of the Information Technology Systems.

(c) should evaluate, categorize and manage all risks emanating from the development, integration and operation of Information Technology Systems. These risks should be evaluated in combination with the rest of the risks to which the institution is exposed.

(d) should ensure that existing policies, prototypes, procedures and methodologies are officially documented and approved by the competent administrative units.

(e) should have standards and methodologies for the design and development of Information Technology Systems as well as procedures for their daily operation, support and monitoring.

(f) should have standards and procedures for the management and the effective completion of information technology projects. The proposal for the development of each major

information technology project should determine the operational objectives as well as the qualitative and quantitative benefits which will be realized by implementing the project.

(g) should guarantee the quality of the information technology services provided via the existence of quality assurance processes and the compliance, at all stages of the product life cycle of systems, with quality standards based on measurable criteria.

(h) should have in place appropriate procedures for the timely identification and effective management of problems emanating from the Information Technology Systems.

(i) should have in place appropriate procedures for the detailed classification, logging and monitoring of events which pose operational risks, including financial losses originating from its Information Technology Systems (eg unauthorized access, theft of computer equipment, fraud, security breaches, non-availability of systems, destruction of computer equipment, malicious use, etc) and the briefing of control functions (Information Security, Risk and Internal Audit), in order to achieve an effective recording and management of operational risk.

(j) should have an appropriate Management Information System, so that the senior management of the institution is effectively informed. Such a system should be based on detailed written procedures and be characterized by a uniform collection and processing of data, timely submission, accuracy, reliability and completeness.

(k) should be aware and comply with the legal, supervisory and regulatory framework for issues related to information technology.

(i) should study, evaluate and apply, where it is considered appropriate, international standards and methodologies for the management and the security of Information Technology Systems. Institutions should also be aware and take into consideration all international developments in the above area.

Organisation of the Information Technology Unit

3. Institutions should establish a specialized, Information Technology Unit, functionally and administratively independent from the end users of the information technology services. This Unit should:

(a) Have an organizational chart according to which:

(i) the operational and organizational needs of the Unit are clearly reflected and the responsibilities of all sub- units are described with clarity,

(ii) the segregation of duties is clearly displayed in order to eliminate the existence of incompatible roles, to facilitate accountability and ensure the utilization of the skills and competences of staff in the most appropriate manner. Especially, the complete

segregation of the functions of design and development of systems from their daily operations should be ensured,

(iii) information technology security staff should be assigned, as necessary, for liaising with the Information Security Officer and ensuring the information security policy is adequately applied to the institution's information technology and network infrastructure,

(iv) it should ensure the replacement of staff, for at least, the critical information technology operations.

(b) Have documented and officially approved terms of reference for all positions, describing the duties, responsibilities and competences required for each position.

Relations with external parties

4. While the employment of the services of external providers may solve important problems, it creates an area of additional risk for the institution, which must be identified, evaluated and managed effectively. Such risks include the possibility of lack of essential control over the services offered, dependence on third parties, loss of internal know-how, potential weakness conferred on the institution to immediately adapt to new requirements by customers or the financial environment, non-transparent pricing of services offered, differences in mentality between the institution and the third party provider;

(a) in the event that the institution decides to outsource any of its information technology services, including its infrastructure, platform, software, or data, to external third party providers, including providers offering "cloud computing" services, then this should be done consciously and in strict compliance with all of the provisions of Appendix 2 of this Directive;

(b) the outsourcing of systems to third parties, which are important to the institution, should be justified by the IT Steering Committee in writing by addressing a report to the institution's senior management, the latter granting its final approval.

PART III

DEVELOPMENT AND COMMISSIONING OF SYSTEMS

5. (1) The life cycle of a system should be characterized by discrete stages which should be implemented based on standards, methodologies and procedures officially documented and approved. The monitoring of the implementation of every important IT project / system should be assigned to the IT Steering Committee. Upon completion of the development of a system, its operational and technical monitoring should be assigned to the corresponding competent units or

executives.

(2) Prior to the development or commissioning of an important system, a feasibility study should be carried out.

Systems Development

6. In the case where an institution decides to develop a new system, or make significant changes to an existing system, it should:

(a) set up a project team prior to launching the project. This team should be assigned with the project management and the preparation of an implementation project plan;

(b) specify in the project plan, inter-alia, the phases, their duration, and the persons in charge for the implementation of each phase as well as the deliverables;

(c) prepare a communication plan specifying the procedures for updating the parties involved with the project's progress;

(d) take into consideration the user acceptance and effective operation criteria for the new information technology system;

(e) address, in detail, the management of the data of any pre-existing system, either automated or manual, by addressing issues such as data cleansing, data conversion and data migration;

(f) during the phases of technical analysis and design, the security requirements of the system should be defined, based on the institution's information security policy and a risk analysis should be carried out for this purpose;

(g) develop the new system in compliance with the applicable standards, in an environment isolated from the production environment;

(h) testing of the new system, at the initial stage, should be conducted by the IT staff in a separate environment. Final testing should be fully documented and integrated and it is essential that, apart from the IT staff, the end users and the Quality Assurance Unit (where applicable) also participate. The Control Functions and the end users should ensure and confirm, prior to the transfer to production, that the requirements set by them have been met;

(i) the transfer of the new system in the production environment should be carried out by specialized staff, such as librarians, based on written procedures;

(j) prior to going live the system should be supported by all necessary documentation in accordance with the standards set by the institution;

(k) users' training should be carried out in a separate environment, isolated from the development and production environment;

(l) the operation and support of the system should include change control procedures, a versioning control system, a procedure for controlling the updates of the system with any necessary patches for fixing errors, a performance monitoring system, procedures for taking and maintaining back-up files, business continuity, briefing of the Help Desk on the support of the users of system, etc;

(m) the discontinuation phase of the system should include procedures for information preservation in accordance with the legal and supervisory requirements. Prior to hardware and software disposal, data should be made unrecoverable.

Systems Commissioning

7. In the case where an institution decides the commissioning of an Information Technology System, it is required that in addition to considering all "Systems Development" requirements, it should take into consideration the following:

(a) The whole process of commissioning should be characterized by separate phases, which should comply with officially documented and approved standards, methodologies and procedures. Such phases are the "Request for Proposal "comprising of a detailed description of the needs which will be covered by the system, the selection procedure of the external supplier, the drafting of the agreement and signing of the contract, integration and operation of systems in the production environment and, finally, the monitoring and control;

(b) the selection of a system must be done based on the detailed business and technical specifications set by the institution;

(c) through an appropriate identification and assessment of risks, that the introduction of new technology features within the information and communication technology infrastructure, does not create additional risks which the institution is not prepared to accept;

(d) the type of any intervention in the system by the institution should be strictly specified beforehand. Any interventions should be based on formally documented and approved procedures and should be carried out by specialized staff. These interventions should be kept to the minimum level possible so that the basic characteristics of the system are not altered, in order to achieve easier maintenance and upgrading. It should be noted that in

the event that there are significant deviations between the functional procedures of the institution and those of the system commissioned, then, normally, the institution should adapt its own procedures to match the system's functional procedures and not the reverse;

(e) any supporting applications which will be extracting information from the institution's main systems for the support of local needs or other operational particularities, should be developed in accordance with the institution's application development standards so that the information systems' homogeneity is preserved;

(f) the systems' support arrangements should be strictly defined and it should be defined, explicitly, in which cases support should be required by the supplier as well as the corresponding response timeframes;

(g) the acquisition of know-how should be pursued, not only through the training of the staff involved in the operation of such systems, but mainly through its involvement in all development stages of the system, so that the dependence of the institution on the supplier is gradually decreased;

(h) provided that the requirements of the institution, as defined in the contract, have been met and after the supplier has conducted and completed all necessary tests, there should be a formal acceptance and delivery procedure whereby the system will be accepted by the institution with the participation of all parties involved

PART IV
OPERATION AND SUPPORT

8. (1) The unhindered operation of Information Technology Systems and their efficient support are crucial factors for the orderly operation of an institution, the development of relations of confidence with customers as well as for the management of operational risk. The prerequisite for the unhindered operation and effective support of an Information Technology System is the compliance with the policies, standards and procedures of the institution by all competent units as well as third party service providers.

Systems Operation

(2) The term "systems operation" refers to the procedures which are necessary for the daily operations of the Information Technology Systems in an institution. In order to have a satisfactory level of secured and efficient operations the following should be in place:

(a) A complete and detailed inventory of information and communication systems equipment, a description of the architecture, the software used as well as versions history, updates and the

usage licenses. A record should also be maintained for all media used for storing and transferring sensitive data;

(b) a complete and updated documentation of each system, including the official handbooks and manuals issued by suppliers of hardware and software systems as well as manuals which are prepared by the institution's staff;

(c) sufficient maintenance and technical support of the systems;

(d) support to end users within the institution as well as of customers. This support should be assigned to a Help Desk facility, suitably organized and staffed;

(e) procedures for the management of the systems' operating parameters;

(f) procedures for the prevention and detection of installation and use of software which is unauthorized by the institution, as well as of any software without having an appropriate license;

(g) planning for the tasks to be completed, recording of problems that may result and the actions to be taken in the event of extraordinary situations. The successful or non-successful completion of scheduled as well as extraordinary tasks which are being carried out should be recorded in an event log-book, along with the signature of the staff which has carried out the activity. The execution of any extraordinary tasks should be carried out only after their execution has been approved and authorized;

(h) checks and controls in order to ensure data integrity, correctness and confidentiality, at all processing stages. Any types of inconsistencies should be identified and managed based on written procedures;

(i) procedures for the management of the capacity, work load and performance of the systems and networks;

(j) continuous monitoring of systems' and networks' availability. More specifically for critical systems, institutions should be in position to calculate their availability rate on an annual basis and compare it with predetermined objectives;

(k) satisfactory procedures for managing back-up copies;

(l) more specifically, for the systems and services which are offered via the internet the following should exist:

(i) Sufficient information should be included on the institution's web-site giving prospective customers adequate information about the identity of the institution and the supervisory

authority which has granted its banking license prior to conducting any transactions electronically. Information should also be given regarding the way customers may contact a support center in the event of problems of any nature, the digital certificate of the web-site which should be issued by a formal certification authority and information for the secure use of the services offered;

(ii) information to customers on the institution's confidentiality policy in relation to their personal data. It is recommended that this information is also available on the institution's web-site. Providing customers the right to deny the disclosure of their personal data to third parties for the promotion of products or other reasons. Customers' data should only be used for the purposes for which customers are aware that it will be used and in line with data protection regulation;

(iii) explicit labeling on the institution's web-site of links to web-sites of other companies or organizations. At all times it should be clear to customers leaving the web-site of the institution that they are being routed to a completely different enterprise or another legal entity;

(iv) automated systems for the monitoring of transactions, whose effective operation will be the basis for the creation, by the institution, of statistical models of customers' transactions. These systems, based on the profile established for each customer, should be in a position to identify any transactions indicating extraordinary behavior and produce, in real time, alerts for the investigation of potential cases of fraud;

(v) effective management of the risk of money laundering and terrorism financing. These risks are particularly enhanced in the electronic transactions as these services are available from anywhere, at any time, also because of the impersonal nature of transactions and their automatic processing. Consequently, institutions are expected to install filters and monitoring tools/systems which, as a minimum, will impose limits on specific groups or categories of transactions, thus, providing the possibility of delaying the execution of a transaction until the verification of specified details etc;

(vi) capability of easily accessing and processing the details of historic transactions, thus, making it feasible to identify particularities and/or irregularities in transactions, which help to establish evidence and provide sufficient information to the supervisory authorities, especially in potential cases of fraud, money laundering, terrorism financing, provision of investment services and other transactions;

(vii) handbooks, in electronic or printed form, which will provide information to customers on how to use the systems with emphasis on security issues. Moreover, institutions should make available to the users information related to best practices for the secure use of personal computers via which they can access the institution's electronic banking and electronic payment systems. The said practices are expected to also make references,

inter-alia, to issues relating to protection from viruses, other malicious software, phishing and other malicious tactics, the secured storage and usage of tokens and personal access codes (specifically when using common access computers. As a matter of principle, however, the usage of such computers should be discouraged and avoided to the extent possible);

(viii) sufficient security procedures with emphasis on the certification of the transacting parties (digital certificate of the web-site of the institution, two level verification for the customer, use of digital certificates or other method), the non-repudiation of transactions, the encryption of communication, the security of transactions (evidence of a successful completion of a transaction, disconnection in the event of an inactive user, identification of suspicious transactions etc), and finally the operation of the systems which support these services in special regions of the network which provide high protection from malicious activity either from internal or exterior users.

Physical Security

(3) The term "Physical Security" refers to the measures which should be taken for the protection of systems and the infrastructure which supports them, from risks that emanate from non-authorized or malignant individuals and environmental disasters. It is essential that an analysis of such risks precedes the implementation of any measures, as it is not possible to have the same security requirements for all the areas and premises which accommodate systems. The physical security measures should include, as a minimum, the following:

(a) Physical access control mechanisms. Such mechanisms should limit, control and record, both the entrance and exit of staff and visitors as well as the movement of computer equipment and storage media. The type of control mechanisms should be defined based on the materiality of the systems they protect. For example, information processing facilities should be provided with the highest level of protection.

(b) mechanisms for the prevention and confrontation of destructions caused by natural disasters;

(c) mechanisms for the prevention and confrontation of malicious actions (burglary / theft, vandalism, terrorist acts, etc). The said risks as well as the risks emanating from natural disasters, apart from the fact that they can cause complete destruction of systems and networks can also endanger the lives of staff;

(d) mechanisms for the prevention and confrontation of problems emanating from the interruption of operations and provision of services, or the damage of supporting units. It is essential that systems operate in appropriate environmental conditions and in a technical

environment which is supported effectively;

(e) the effective management of telecommunications and network wiring for the confrontation of issues, such as material deterioration, interference and lack of suitable labeling;

(f) mechanisms for the security of portable systems. The use of portable computers and any other mobile devices should be taken into consideration, seriously, when carrying out a risk analysis. Portable computers and mobile devices which hold sensitive corporate data should be securely stored when not in use and, furthermore, sensitive data stored onto them should be in an encrypted form;

(g) the secured transfer and storage of documents and removable media holding sensitive information. The former category includes, among others, classified reports, password back-up copies for the systems administrators, customer passwords until they are dispatched to them, documentation of systems and applications, the Information Security Policy, the Business Continuity and Disaster Recovery Plans. The latter category includes, among others, data back-ups and plastic card material;

(h) the selection and suitable configuration of the premises in order to minimize the above risks, in relation to the intended usage and the criticality of the systems installed therein.

Logical security

(4) The term “logical security” refers to the measures taken for the restriction of access to systems resources. System resources are considered to be the computer equipment and networks, both physical and virtual, software and data. The measures implementing the logical security define not only “who” or “what” (eg which program) will have access to specific resources of a system, but also the type of the permissible access. These measures may be incorporated in the operating systems, implemented within applications, in database management systems, in communications systems or may be implemented through the usage of additional standalone security software packages. For the maintenance of a satisfactory level of logical security, it is necessary that:

(a) for the safety of accessing the systems

(i) all users have a unique individual access account for each system and only for those resources that they are eligible to access, so that each action can be uniquely traced. Consequently, common / group access accounts should not be used and, in case where this is not feasible, then the activities of these accounts should be closely monitored and controlled;

(ii) where system / service access accounts must be used, their purpose shall be

adequately documented and strict security measures shall be applied for access to these accounts;

(iii) the management of accounts, the designation and revision of access rights granted to each account should be described in written and approved procedures. Furthermore, the segregation of duties must be enforced in the approval, implementation and reviewing of access rights;

(iv) any activities carried out through a privileged account, such as the system's administrator account or the accounts of users with extended privileges, should be recorded and monitored closely;

(v) accounts should be deactivated immediately when they are no longer necessary or in cases of a serious security violation incident;

(vi) a specific procedure should be in place for the creation of temporary accounts with pre-defined privileges for carrying out specific tasks or in cases of emergency. The use of these accounts should be closely monitored and checked and as soon as the need for which they were created ceases, they should immediately be deactivated;

(vii) when accessing the system, the owner of an account should be appropriately authenticated based on secure, up-to-date best practice methods;

(viii) any default passwords set by the suppliers for any new system or equipment delivered should be changed immediately;

(ix) passwords, commensurate to the criticality of information they protect, should:

1. be created and based on up to date best practice standards;
2. be managed based on policies and procedures.;
3. be kept confidential. This responsibility lies with the holder.
4. be changed periodically. A change must be enforced the first time a user enters a system.

(x) the back-up copies of the system administrators' access codes or those of special privileges accounts must be kept at a secured a location and access to them, in a case of emergency, should be granted following a special procedure;

(xi) in cases where it is considered appropriate, access codes for accounts with special privileges may not be kept as a whole but in parts, having each part under the custody of a different person;

(xii) wherever feasible, special software should be used for the management and control of access;

(b) for the protection of data

(i) the various systems should have inbuilt data controls and, more specifically, at the preparation, input and processing stages;

(ii) there should be a documented and approved procedure for classifying data based on its degree of sensitivity. For more sensitive data, handling and processing procedures should be based on additional security requirements,such as encryption techniques and other methods of protection.

(iii) by means of encryption:

1. it should be clearly defined when and at what level encryption should be applied;
2. a high security encryption key should be used across all software;
3. an appropriate encryption algorithm should be used, based on its type, strength, and quality;
4. a public key infrastructure should be in place for the management of digital certificates, mainly for the communication of the institution with its customers when using electronic banking services;
5. conformity should be sought with the national and international regulations and practices of encryption.

(iv) all necessary measures should be taken in order to comply with the relevant legislation and data protection regulations;

(v) there should be in place a policy for informing customers in the event that there is a leakage of their confidential personal data due to a system security breach;

(vi) for databases

1. there should exist a complete and precise documentation of the database which, as a minimum, should include the logical design, the physical design and the data dictionary;
2. a reorganization of the database should be carried out on a regular basis;
3. It should be ensured that only completed transactions are recorded in the database ("commit/rollback").

(c) for the systems protection

(i) software for the protection from viruses or other malicious software should be installed and kept up-to-date;

(ii) the sensitive resources of the systems, such as system and application files should be protected in an effective manner;

(iii) a file should be maintained for recording all software approved by the institution;

(iv) any software or function not required on any system should be de-installed or deactivated, if it is not used;

(v) auditing and logging functions should be enabled in each system and appropriate parameters should be set in cooperation with the internal audit;

(vi) it should be ensured, wherever necessary, and based on an approval procedure, that

systems are updated with the most recent versions and updates of software and patches related to security issues so that their weaknesses and vulnerabilities are minimized;

(vii) documented procedures should exist for restoring the security of the system in the event that there is a security breach;

(viii) electronic mail should be protected, wherever feasible, from risks such as tapping and / or alteration of its contents, non-authenticated senders, malicious attachments, unwanted messages;

(ix) restrictions should be imposed on the permissible activities when using the internet, for example accessing certain web sites, transferring data and other similar activities ;

(x) users should be trained, on a continuous basis, on issues related to the secure use of the systems;

(xi) critical systems should be protected effectively from malicious activities by external or internal users. To the above end special techniques may be used such as:

1. The use of specialized systems (firewalls, filtering routers etc), which, control the entry points and manage and control communications to and from areas of the network which are normally more exposed to risks;
2. The creation of “Demilitarized Zones” between the entry control points which act as an isolated network for the accessible systems of an institution, by internal or exterior users, thus, protecting effectively the remainder network from malicious actions.

(d) for the security of the network infrastructure and communications

(i) The communication gateways with external networks should be clearly identified, recorded and controlled;

(ii) for better access control, network segmentation into controlled sub-networks should be considered;

(iii) no ports should remain open on any device on the network apart from those explicitly specified that are required for the services supported, after the risk involved by keeping them open has been assessed;

(iv) access to special functions for the management and control of the network should be limited and adequately controlled;

(v) setting of parameters in the various network devices should be effectively managed;

(vi) the network administrator should have the capability of identifying any unauthorized devises on the network;

(vii) access points located in areas where physical access is not controlled should be limited to the absolute minimum. When they are not used they should be disabled;

(viii) wireless connection capabilities to the network should be limited and closely monitored in order to deter intrusion attempts by unauthorized users;

(ix) remote login facilities should not be made available; however, in cases where such a facility is necessary, it should be recorded and closely monitored;

(x) appropriate communication protocols should be used depending on the type of data that is transmitted, addressing effectively data management and security issues;

(xi) the confidentiality and integrity of data transmitted on the network should be ensured for the whole route;

(xii) vulnerability tests should be carried out using specialized software tools in order to identify security gaps or areas with deteriorating security;

(xiii) intrusion detection/prevention systems should be activated on the network in order to identify any intrusion attempts or any attempts to breach security;

(xiv) external and internal penetration tests, based on predefined scenarios, should be carried out on a regular basis by specialized external third parties in order to assess the adequacy of the network's security;

(xv) any technical threats and vulnerabilities should be identified, evaluated and treated in a timely manner through the establishment of an appropriate vulnerability management programme.

Business continuity and disaster recovery plans

(5) Institutions should establish a sound business continuity management programme to ensure their ability to operate on an on-going basis and limit losses in the event of severe business disruption. Within this scope, institutions should have a Business Continuity Plan in place, which must be approved by senior management, so that the continuity of the most critical functions and Information Systems is ensured. Moreover, institutions should have effective Disaster Recovery Plans which will be activated in the event of devastating incidents which may cause extended disruption to the operation of a critical system, the entire computer centre or even the entire Information Technology infrastructure. In order to establish sound Business Continuity and Disaster Recovery Plans, institutions should carefully analyze their exposure to severe business disruptions and assess (quantitavely and qualitatively) their potential impact, using internal and/or external data and scenario analysis. This analysis should cover all units of the institution and take into account their interdependency. Based on these:

(a) all critical functions should be defined as well as the systems and resources they will use.

(b) the recovery priorities and objectives should be clearly set out.

(c) all risks threatening critical operations should be identified and be classified according to their probability of occurrence and their probable impact on systems and functions.

(d) the operational cost from a potential interruption of critical operations and the cost of

activation of a Business Continuity Plan and the Disaster Recovery Plan should be calculated in order to determine the conditions under which the corresponding plan will be activated.

(e) the recovery time and the recovery point of the critical applications should be defined.

(6) The first stage of ensuring business continuity is the existence of a plan for taking and managing back-up copies of the software, data, the systems' parameters as well as the existence of the necessary back-up equipment, such as UPS devices and power generators at the premises where the systems are installed. Aiming at a quick and successful recovery of data and software, taking back-up copies should be done under the following specific procedures:

(a) copies should be taken at a frequency dictated by the importance of information stored.

(b) safe storage within the systems area.

(c) safe transport and storage at a remote location of additional copies.

(d) testing to ensure data integrity.

(e) record keeping including the recording of the contents and the retention period.

(7) At a second stage, a complete and effective Business Continuity Plan and a Disaster Recovery Plan are recommended which should be written in simple and comprehensible language and be communicated officially to all staff involved. Any classified information contained in the plan such as access codes, security keys, network diagrams and other relevant information, should be disclosed only to duly authorized staff. A copy of the plan should be physically stored in secured areas and on systems physically separated from the computer centre. In addition, it should be readily accessible by involved staff in case of emergency. Such a plan should include:

(a) A classification of systems based on functional needs. Such classification should, inter-alia, include the required recovery time and the minimum estimated performance of each system after recovery;

(b) the explicit hierarchical structure of all executives participating in its implementation, their competences as well as the persons in charge of decision-making in each emergency team;

(c) the procedures for estimating the extent of the destruction. Based upon this estimate, those parts of the plan which have to be activated should be identified;

(d) the procedures for activating the plan, notifying the executives and mobilizing the emergency teams;

(e) the tasks which will be executed when specific emergencies occur, which, inter-alia, should protect the staff in cases of danger / disaster (eg fire, earthquake etc);

(f) the alternative working stations of users, the equipment that will be used as well as their corresponding specifications;

(g) the procedures for the preparation and activation of the alternative computer centre;

(h) the systems of the alternative centre, its infrastructure including the topology of the network;

(i) a list of suppliers with which there are contracts, the services offered by them and the expected response times in the event of an emergency;

(j) the procedures which should ensure that the plans are maintained, revised and updated whenever there are changes in the procedures of the institution;

(k) the procedures for training the staff, according to the duties assigned to them, when the plan will be implemented;

(l) the procedures for carrying out tests, according to which:

(i) the test frequency should be defined (at least once a year).
(ii) clear objectives should exist beforehand, for both the testing of specific subsystems and for the testing of the system as a whole. Testing the latter includes covering completely all critical operations as they are recorded in the plan and using exclusively the contingency site, equipment and back-up copies.
(iii) tests should be conducted under conditions simulating an emergency situation.
(iv) the participation of the Internal Audit Unit should be ensured.
(v) a report should be prepared after the conclusion of the tests.
(vi) plans should be reviewed and revised in order to address all challenges and failures observed in each test.
(vii) the outcome of the tests should be communicated to senior management and the Audit Committee.

(8) Finally it should:

(a) ensure the existence of appropriate recovery plans for critical resources to enable the institution to return to normal business procedures in an appropriate timeframe;
(b) ensure the effective operation of the contingency computer centre, which should be located at a suitable distance, so that it will not be affected by the same risks that may affect the main computer centre. The contingency site should be equipped with suitable (back-up) equipment that should provide all critical services within the time limits set as well as

procedures manuals and user instructions for the systems. Moreover, it should allow for the unhindered use of the alternative equipment up to the time when operations will be recovered in the main computer centre;

(c) ensure the physical security of the contingency site as well as a reasonable level of logical security during the implementation of the plan.

(d) ensure that the institution is covered, through appropriate insurance, against the risks which could possibly cause the interruption of operations of its Information Technology Systems.

(e) In the event that the premises of the contingency site, the equipment or services are provided by a third party:

(i) Appropriate contractual agreements should ensure the efficient continuation of operations in the event that a disaster affects simultaneously many organizations serviced by the same third party service provider.

(ii) The third party service provider should be informed of any changes in the systems which are likely to require corresponding adaptations to Disaster Recovery Plans.

PART V
AUDIT OF INFORMATION TECHNOLOGY SYSTEMS

9. (1) An effective audit function for the Information Technology Systems should focus on the risks emanating from their development, integration and operation, examine the adequacy of controls and procedures and propose, where needed, appropriate modifications. Moreover, it should evaluate the extent of compliance with corporate strategy and policies, standards and procedures and should also follow-up the degree of compliance with the observations of the audits carried out. Finally, it should have a complete overall picture of the Information Technology Systems operation enabling it to provide satisfactory information, on an annual basis, to the Audit Committee.

(2) For the above reasons, the Internal Audit Function is expected:

(a) to have the know-how, the qualitative and quantitative adequacy of staff, resources and procedures in order to carry out specialized audits of the Information Technology Systems. The know-how and the staff training should be such that all current and future audit requirements of the computerized functions of the institution are covered;

(b) to prepare and carry out an audit plan, which will be based on the risk analysis carried out in relation to the Information Technology Systems as well as on the findings of previous audits;

(c) to follow written procedures for the planning, organization and conduct of audits, report of conclusions as well as procedures for the follow-up. The above procedures, the various audit work programmes used in these specialized audits as well as the methodology used

for analyzing the automation risks, should constitute the official documentation of the audit function of Information Technology Systems;

(d) to follow-up issues which concern the Information Technology Systems of the institution, so that it can form an opinion on the existing risks or the risks which may emerge. For the purposes of forming a conclusive opinion and, to the maximum extent possible, it is recommended that the Internal Audit Function monitors the operations of the Information Technology Systems through special, non-operational access rights, participates in project committees and puts in place mechanisms for being immediately informed of any material problems and incidences;

(e) to make use – on a case by case basis – of specialized auditing software for a more effective audit of the systems' security and the integrity of their data;

(f) to participate during the phase of designing systems for the designation of appropriate internal controls necessary for information systems audit, and for defining the audit trail files and reports to be produced for facilitating audit and control. It should also participate in the testing phase;

(g) to check and evaluate the procedures which produce information submitted to the senior management of the institution and the supervisory authorities in order to ensure their completeness and accuracy.

(h) to inform immediately and in detail the Central Bank of Cyprus, in the case of a serious problem or an extraordinary incident involving the Information Technology Systems (cases of fraud, security breaches of important systems, non-availability or the malfunctioning of critical systems, activation of Disaster Recovery Plans), or in the case of invocation of its Business Continuity Plan following a disaster.

(i) to check and evaluate the adequacy of and conformity to procedures which control all phases of cooperation of the institution (choice of third party, contracting and execution of the contract, quality of services provided) with suppliers and third party computer services providers, based on the requirements of Part III of this Appendix;

(j) to supervise the audit activity of information technology at a group level. For this purpose it is expected to maintain communication channels in order to achieve an effective cooperation with the management and the Internal Audit Functions of subsidiary companies and the branch network abroad. To evaluate the adequacy of the audit work done through the submission of periodic reports or even through the participation in the Audit Committee of the subsidiaries, especially in those cases where the size and the complexity of systems make it necessary. To evaluate the adequacy of specialized audits carried out by internal and external auditors. To carry out routine or special audits, depending on the circumstances, in order to cover auditing needs which are not covered sufficiently by the Internal Audit Functions in question or when they are considered essential based on a risk

analysis;

(k) to study, evaluate and apply, where considered appropriate, international standards and methodologies for auditing an Information Technology System.

(3) With regard to the audit carried out by external auditors, institutions should have a policy regarding the extent and the role of external audit on their Information Technology Systems as well as procedures for evaluating the services offered. The above policy should clarify and document those cases where the external auditor acts in parallel with the Internal Audit Function offering an additional specialized opinion or where it acts in a complementary manner in order to cover specialized audit requirements which cannot be covered internally or where both cases above apply.