ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

To : **Regulated Entities**
- **i. Cyprus Investment Firms**
- **ii. UCITS Management Companies**[1]
- **iii. Alternative Investment Fund Managers**[2]

FROM : **Cyprus Securities and Exchange Commission**

DATE : **10 March 2015**

CIRCULAR No. : **C056**

SUBJECT : **Internal audit function**

The Cyprus Securities and Exchange Commission ('the CySEC') wishes, with this circular, to inform the Regulated Entities on certain aspects of the internal audit function.

A. Regulatory Framework

Cyprus Investment Firms

1. According to section 18(2)(f) of the Investment Services and Activities and Regulated Markets Law of 2007, as in force ('the Law') *«A CIF must have sound internal control mechanisms.»*

2. According to paragraph 8 of the Directive DI144-2007-01 of 2012 ('the Directive') *«A CIF is required, where appropriate and proportionate, taking into account the nature, the scale and the complexity of its business activities, as well as the nature and the range of its investment services and activities, to establish and maintain an internal audit function which is separate and independent from the other functions and activities of the CIF and which has the following responsibilities:*

[1] This Circular applies to UCITS Management Companies when providing investment services
[2] This Circular applies to Alternative Investment Fund Managers when providing investment services

(a) *to establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the CIF's systems, internal control mechanisms and arrangements;*
(b) *to issue recommendations based on the result of work carried out in accordance with point (a);*
(c) *to verify compliance with the recommendations of point (b);*
(d) *to report in relation to internal audit matters in accordance with paragraph 9(2).»*

UCITS Management companies

3. According to section 109(6) of the Open-Ended Undertakings for Collective Investment Law *«The Investment Services and Activities and Regulated Markets Law shall apply to the provision of the services[3] referred to in subsection (4) by the Management Company.»*

Alternative Investment Fund Managers

4. According to section 6(8) of the Alternative Investment Fund Managers Law *«Sections 3(3), 10, 18, 36 and 77(6) of the Investment Services and Activities and Regulated Markets Law shall apply to the provision of the services[4] referred to in paragraph (6) of this section by AIFMS.»*

5. This circular should be read together with the proportionality principle as set out in paragraph 8 of the Directive (the establishment and maintenance of a separate and independent internal audit function is not compulsory for all Regulated Entities).

B. Scope of activity – Responsibilities of the internal audit function

6. Every activity (including outsourced activities) of the Regulated Entity should fall within the overall scope of the internal audit function.

7. Internal audit's scope should be unrestricted. In setting its scope, internal audit should independently determine the key risks that the Regulated Entity faces, including emerging and systemic risks, and how effectively these risks are being managed. There should be no impediment to internal audit's ability to challenge the senior management and to report its concerns.

8. In particular, the internal audit function should independently examine and evaluate the:

i. Effectiveness and efficiency of internal control, risk management and governance systems and process in the context of both current and potential future risks;

[3] Portfolio management and investment advice
[4] Portfolio management, investment advice, reception and transmission of financial instruments

ii. Reliability, effectiveness and integrity of management information systems and processes (including relevance, accuracy, completeness, availability, confidentiality and comprehensiveness of data);

iii. Monitoring of compliance with laws and regulations, including any requirements from CySEC and other supervisors, where relevant (with emphasis whether the Regulated Entity is acting with integrity in its dealing with all clients and in its interaction with relevant markets); and

iv. Safeguarding of assets.

9. The Internal Auditor is responsible for establishing, implementing and maintaining an internal audit plan governing all the above aspects. Internal audit should make a risk-based decision as to which areas within its scope should be included in the audit plan – it does not have to cover all the potential scope areas every year provided that this is clearly justified.

In setting its priorities and deciding where to carry out more detailed work, internal audit should focus on the areas where it considers risk to be higher, as well as taking into account the wishes of the board of directors. Both the determination and the assessment should be informed, but not driven, by the views of board of directors or the risk management function.

The audit plan should be updated at least annually (or more frequently to enable an ongoing real-time assessment of where significant risks lie).

10. The Internal Auditor should ensure adequate coverage of matters of regulatory interest within the audit plan. In particular, based on the results of the risk based assessment, the Internal Auditor should undertake reviews of key risk management functions, regulatory capital adequacy functions, regulatory and internal reporting functions, the regulatory compliance function and the finance function. More specifically, the Internal Auditor should review, among others, the following:

i. *Risk management*

A Regulated Entity's risk management processes support and reflect its adherence to regulatory provisions and safe and sound investment services practices. Therefore, internal audit should include in its scope aspects such as:

- the organisation and mandates of the risk management function,
- evaluation of risk appetite, escalation and reporting of issues and decisions taken by the risk management function,
- the adequacy of risk management systems and processes for identifying, measuring, assessing, controlling, responding to, and reporting on all the risks resulting from the Regulated Entity's activities,
- the integrity of the risk management information systems, including the accuracy, reliability and completeness of the data used, and

- the approval and maintenance of risk models including verification of the consistency, timeliness, independence and reliability of data sources used in such models.

ii. *Capital adequacy*

Regulated Entities are subject to regulatory framework for capital. The framework contains measures to strengthen regulatory capital. The scope of internal audit should include all provisions of this regulatory framework and in particular the Regulated Enity's system for identifying and measuring its regulatory capital and assessing the adequacy of its capital resources in relation to the Regulated Entity's risk exposures and established minimum ratios.

iii. *Regulatory and internal reporting*

The Internal Auditor should regularly evaluate the effectiveness of the process by which the risk and reporting functions interact to produce timely, accurate, reliable and relevant reports for internal use and the CySEC.

iv. *Compliance*

The scope of the activities of the compliance function should be subject to periodic review by the internal audit function. The audit of the compliance function should include an assessment of how effectively it fulfils its responsibilities.

v. *Finance*

A Regulated Entity's finance function is responsible for the integrity and accuracy of financial data and reporting. Key aspects of finance's activities have an impact on the level of the Regulated Entity's capital resources and therefore associated controls should be robust and consistently applied across similar risks and businesses. As such, it is important that these controls are subject to periodic internal audit review, using resources and expertise to provide an effective evaluation of Regulated Entity practices.

11. The Internal Auditor should promptly inform the senior management about his findings; issue recommendations to these persons based on the results of the work carried out and verify compliance with these recommendations.

12. The Internal Auditor must, at least annually, prepare an internal audit report, which it is addressed to the board of directors and senior management.

13. The Internal Auditor is responsible for the internal audit function, and for any reports prepared. In case of outsourcing the internal audit function, the responsibility lies with the service provider (physical person) and in no case the responsibility is limited through the outsourcing agreement.

C. Internal Audit Report ('the Report')

14. The aim of the Report is to provide an independent assurance to the board of directors and senior management on the quality and effectiveness of the Regulated Entity's internal control, risk management and governance systems and processes.

15. The Report should, at least, include the following:

i. An overall description of the internal control, risk management and governance systems and process established by the Regulated Entity.

ii. A description of the audit plan and the risk-based approach followed.

iii. A summary of:

- regular and/or extraordinary audits (on-site or desk-based) carried out,
- major audit findings/weaknesses identified,
- recommendations made in relation to audit findings/weaknesses identified,
- management response including the actions taken on the major audit findings/weaknesses and recommendations,
- any outstanding issues for which the management response was not satisfactory or no actions have been taken,

iv. A follow up on the outstanding issues of the last report.

v. Other significant internal audit issues that have occurred since the last report.

16. The Report must be submitted to CySEC along with the minutes of the Board of Directors' meeting during which the Report has been discussed within twenty days from the date of the relevant meeting and not later than four months from the end of the calendar year [paragraph 9 (4) of the Directive].

It is provided that the Report submitted to the CySEC is the same with the one discussed at the Board of Directors' meeting.

The minutes of the Board of Directors' meeting must explicitly state the corrective measures to be taken with respect to the audit findings/recommendations mentioned in the Report, as well as a timetable for their implementation.

D. Record keeping

17. The Internal auditor is required to record all relevant information about the audits carried out.

18. The Internal audit records must be kept at the head office of the Regulated Entity and be available for inspection by the CySEC, whenever it is requested.

E. Responsibilities of the Regulated Entity's board of directors

19. The Regulated Entity's board of directors has the ultimate responsibility for ensuring that an adequate, effective and efficient internal control system has been established and maintained. It must also be satisfied as to the effectiveness of the Regulated Entity's internal audit function, that policies and procedures are followed and that senior management takes appropriate and timely corrective action in response to internal audit weaknesses identified by the Internal Auditor.

Regardless of whether internal audit activities are outsourced, the board of directors remains ultimately responsible for the internal audit function and in addition, it maintains adequate oversight on the service provider and ensures that the provisions of Part V of the Directive are applied at all times.

20. At least once a year, the board of directors should review the effectiveness and efficiency of the internal control system based, in part, on information provided by the internal audit function (e.g. through the Report). Moreover, as part of their oversight responsibilities, the board of directors should review the performance of the internal audit function.

F. Duties of senior management

21. Senior management should inform the internal audit function of new developments, initiatives, projects, products and operational changes and ensure that all associated risks, known and anticipated, are identified and communicated at an early stage.

22. Senior management should ensure that timely and appropriate actions are taken on all internal audit findings and recommendations.

23. Senior management should ensure that the Internal Auditor has the necessary resources, financial and otherwise, available to carry out his or her duties commensurate with the annual internal audit plan.

G. Independence of the internal audit function

24. The internal audit function must be independent of the audited activities, which requires the internal audit function to have sufficient standing and authority within the Regulated Entity, thereby enabling internal auditors to carry out their assignments with objectivity.

25. The internal audit function must be able to perform its assignments on its own initiative in all areas and functions of the Regulated Entity. It must be free to report its findings and assessments internally through clear reporting lines.

26. The internal audit function should not be involved in designing, selecting, implementing or operating specific internal control measures. However, the independence of the internal

audit function should not prevent senior management from requesting input from internal audit on matters related to risk and internal controls. Nevertheless, the development and implementation of internal controls should remain the responsibility of senior management.

27. The independence and objectivity of the internal audit function may be undermined if the Internal Auditor's remuneration is linked to the financial performance of the business lines for which they exercise internal audit responsibilities.

28. Where a Regulated Entity considers that it is not appropriate and proportionate to establish and maintain a separate and independent internal audit function and makes use of the proportionality exemption laid down in paragraph 8 of the Directive, it should record how this is justified, so that the CySEC is able to assess this. The Regulated Entity should review regularly the above and verify that the proportionality exemption is still applied.

H. Professional competence and due professional care

29. Professional competence, including the knowledge and experience of the internal auditor is essential to the effectiveness of the Regulated Entity's internal audit function.

I. Reporting lines of the internal audit function

30. The internal audit function should be accountable to the board of directors on all matters related to the performance of the internal audit function.

J. The relationship between the internal audit, compliance and risk management functions

31. The relationship between a Regulated Entity's business units, the support functions and the internal audit function can be explained using the *three lines of defence* model.

The business units are the first line of defence. They undertake risks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks of their business.

The second line of defence includes the support functions, such as risk management, compliance, legal, human resources, finance, operations, and technology. Each of these functions, in close relationship with the business units, ensures that risks in the business units have been appropriately identified and managed. The business support functions work closely to help define strategy, implement Regulated Entity's policies and procedures, and collect information to create a Regulated Entity-wide view of risks.

The third line of defence is the internal audit function that independently assesses the effectiveness of the processes created in the first and second lines of defence and provides assurance on these processes.

Line of defence	Examples	Approach
First line	Front Office, any client-facing activity	Transaction-based, ongoing
Second line	Risk Management, Compliance, Legal, Human Resources, Finance, Operations, and Technology	Risk-based, ongoing or periodic
Third line	Internal Audit	Risk-based, periodic

32. The responsibility for internal control does not transfer from one line of defence to the next line.

K. Relationship with CySEC

33. The Internal Auditor should have an open, constructive and co-operative relationship with CySEC which supports sharing of information relevant to carrying out their respective responsibilities.

34. The disclosure in good faith to CySEC does not constitute a breach of any contractual or legal restriction on disclosure of information and does not involve such person in liability of any kind.

The CySEC expects that all Regulated Entities fully comprehend the importance of the internal audit function and take every possible measure for full and continuous compliance with their obligations emanated by the relevant legislation.

Sincerely,

Demetra Kalogerou
Chairman of the Cyprus Securities and Exchange Commission