ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

| | |
|---|---|
| **TO** | **: Cyprus Investment Firms (CIFs)** |
| **FROM** | **: Cyprus Securities and Exchange Commission** |
| **DATE** | **: 18 December 2023** |
| **CIRCULAR NO.** | **: C609** |
| **SUBJECT** | **: EBA Guidelines on Information and Communication Technology (ICT) and security risks management (EBA/GL/2019/04)** |

Following the Cyprus Securities and Exchange Commission (the "CySEC") Circular C571 regarding the EBA Guidelines on Information and Communication Technology (ICT) and security risks management (EBA/GL/2019/04) (the "Guidelines"), CySEC would like to clarify the following:

1. According to paragraph 11 of the Guidelines, CIFs should assign the responsibility for managing and overseeing ICT and security risks to a control function.

   This control function may be outsourced if appropriate and proportionate to the nature, scale and complexity of the risks inherent in the business model and the activities of the CIF as detailed in section 20(3) of Law 165(I)/2021 and as specified further in Title I of the EBA Guidelines on internal governance under Directive (EU) 2019/2034 (EBA/GL/2021/14).

2. Paragraph 11 in section 3.3. "ICT and security risk management framework" of the Guidelines states that:

   «*The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security related activities and units of a financial institution with the financial institution's policies and procedures and with external requirements, adhering to the requirements of Section 20 of the EBA Guidelines on internal governance under Directive (EU) 2019/2034 (EBA/GL/2021/14)*[1]*».*

[1] CIFs should consider the EBA Guidelines on internal governance under IFD and not the EBA Guidelines under CRD (EBA/GL/2017/11).

The internal audit function mentioned above is the appointed internal auditor of the CIF and it is anticipated that it has the capability to comprehensively assess the ICT and security aspects of the CIF within the scope of its audit responsibilities and prepare the internal audit report accordingly.

3. Paragraph 25 of the Guidelines states that:

«*A CIF's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the CIF. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks».*

The audit mentioned above may be performed by the internal auditor of the CIF or another auditor appointed by the CIF. An independent assurance report conducted either by the internal auditor or another auditor should be generated. This separate report aims to provide independent assurance of the effectiveness of the CIF's governance, systems, and processes in addressing ICT and security risks, providing valuable insights to the management body.

Sincerely,

Dr. George Theocharides
Chairman
Cyprus Securities and Exchange Commission