ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

TO	**: Cyprus Investment Firms (CIFs)**
FROM	**: Cyprus Securities and Exchange Commission**
DATE	**: May 2, 2023**
CIRCULAR NO.	**: C571**
SUBJECT	**: EBA Guidelines on Information and Communication Technology (ICT) and security risks management (EBA/GL/2019/04)**

1. The Cyprus Securities and Exchange Commission (the "CySEC") wishes to bring the attention of the Cyprus Investment Firms (the "CIFs") the Guidelines on ICT and security risk management (the 'Guidelines'). It is noted that the Guidelines were published on November 29, 2019 by the European Banking Authority (EBA).

2. CySEC has adopted the Guidelines, under section 20 of the Prudential Supervision of Investment Firms Law of 2021, which transposes Article 26 of the Directive (EU) 2019/2034[1] (the "IFD") and under Article 74 of Directive 2013/36/EU (CRD), by incorporating them into its supervisory practices and regulatory approach.

3. The Guidelines apply to CIFs that fall under sections 9(1), (3) and (4) of the Prudential Supervision of Investment Firms Law of 2021, ie. with initial capital requirement of €150.000 and €750.000.

4. The Guidelines address ICT and security risks that have increased in recent years. This is due to the increasing digitalisation of the financial sector and the increasing interconnectedness through telecommunications channels (internet, mobile and wireless lines, and wide area networks) and with other financial institutions and third parties. This renders financial institutions' operations vulnerable to external security attacks, including cyber-attacks; therefore, recognising the need for preparedness for cybersecurity, these guidelines implicitly cover the need for cybersecurity within the financial institution's information security measures. While the Guidelines recognise that cybersecurity should be undertaken as part of a financial institution overall information security risk management. Particularly, the Guidelines specify the risk management measures that financial institutions must take to manage their ICT and security risks for all activities.

5. Among others the Guidelines specify the following:

i. The management body of a CIF should ensure that it has adequate internal governance and internal control framework in place for its ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security

[1] Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU {OJ L 314 5.12.2019, p. 64}.

risk management, and business continuity, including those for the management body and its committees.

ii. A CIF should assign the responsibility for managing and overseeing ICT and security risks to a control function, adhering to the requirements of Section 19 of the EBA Guidelines on internal governance (EBA/GL/2017/11).

iii. The 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 frequency and focus of such audits should be commensurate with the relevant ICT and security risks. The management body of the CIF should approve the audit plan, including any ICT audits and any material modifications thereto.

6. Therefore, CySEC expects that:

i. The CIFs[2] will take the necessary actions to ensure compliance with the Guidelines the soonest possible, **and not later than 31.12.2023,** if they haven't already done so. Specifically:

- The CIFs should determine their governance and internal control framework for their ICT and security risks that would be approved by their Board of Directors and establish measures to manage and mitigate their ICT and security risks.
- The CIFs should assign to their internal audit function to independently review and provide objective assurance of the compliance of all ICT and security related activities and units of the CIF with its policies and procedures, adhering to the requirements of Section 22 of the EBA Guidelines on internal governance (EBA/GL/2017/11).
- The Board of Directors of the CIF should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the CIF and should be updated regularly.

The first internal audit report regarding the review of the CIFs' compliance of all ICT and security related activities with its policies and procedures and with external requirements should be submitted to their Board of Directors **by 30.6.2024, the latest.** The internal audit reports should be available for submission to CySEC upon request.

Sincerely,

Dr. George Theocharides
Chairman
Cyprus Securities and Exchange Commission

[2] Initial capital requirement €150.000 and €750.000