ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

TO : **Regulated Entities:**

i. **Cyprus Investment Firms ('CIFs')**
ii. **Central Securities Depositories**
iii. **Trading Venues**
iv. **Crypto-Asset Providers (CASPs)**
v. **Alternative Investment Fund Managers ('AIFMs')**
vi. **UCITS Management Companies ('UCITS')**

FROM : **Cyprus Securities and Exchange Commission**

DATE : **19 January 2026**

CIRCULAR No : **C751**

SUBJECT : **Digital Operational Resilience Act – Reporting, Governance and Portal-related obligations**

Following Circular C700, the Cyprus Securities and Exchange Commission (the '**CySEC**') hereby issues this Circular to provide guidance to Regulated Entities in relation to certain obligations arising under Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (the Digital Operational Resilience Act – '**DORA**'):

A. Major ICT-Related Incident Reporting

1. CySEC has observed deficiencies in the classification and reporting of ICT-related incidents by Regulated Entities. In particular, incidents that should be classified and reported as major ICT-related incidents have not been reported, while in other cases incidents that were reported were incorrectly classified as major.

2. Regulated Entities are therefore required to carefully consult the Commission Delegated Regulation 2024/1772 on the criteria of the classification of ICT-related incidents and cyber threats, which sets out the applicable materiality thresholds and specifies the content and format of reports of major ICT-related incidents. Regulated Entities should also take into consideration the diagram included in the Annex thereto, as discussed in the Final report accompanying the relevant Regulatory Technical Standards, in order to ensure the correct classification and timely reporting of major ICT-related incidents upon detection.

B. Register of Information - Submission format

3. As communicated in Circular C719, CySEC has discontinued the submission of the "Build in Excel" file via its XBRL portal. Consequently, Regulated Entities are required to submit the Register of Information in XBRL-CSV format, which is the only format accepted by the European Banking Authority (EBA).

4. Regulated Entities shall use XBRL Compatible Software that supports mapping and validation against EBA rules and enables the generation of fully compliant XBRL files. The XBRL files shall be compressed (zipped) and submitted through the CySEC XBRL Portal.

5. Regulated Entities are reminded that the Register of Information must be submitted to CySEC on an **annual basis, no later than 28 February of each year, with reference date 31 December of the year preceding the reporting date**.

C. ICT risk management framework

6. Regulated Entities are reminded of the requirements set out in Article 6 of DORA concerning the ICT risk management framework, including the obligation to establish, implement and maintain a well-documented framework that enables effective and continuous management of ICT risks.

7. Pursuant to Article 6(4) of DORA, financial entities[1] other than microenterprises, shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of that function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence between ICT risk management functions, control functions and internal audit functions, according to the three lines of defence model, or an equivalent internal risk management and control framework.

8. Pursuant to Article 6(5) of DORA, the ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, following supervisory instructions or following conclusions derived from relevant digital operational resilience testing or audit processes. The framework shall be continuously improved based on lessons learned from its implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to CySEC upon request. The Report on the ICT risk management framework review should be based on the Chapter V of the Commission Delegated Regulation (EU) 2024/1774.

9. Pursuant to Article 6(6) of DORA, the ICT risk management framework of financial entities, other than microenterprises, shall be subject to internal audit by auditors on a regular basis in line with the financial entities' audit plan. Those auditors shall possess

[1] Any reference in DORA to 'financial entities' shall, for the purposes of this Circular, be understood as a reference to the Regulated Entities.

sufficient knowledge, skills and expertise in ICT risk, and shall operate with an appropriate level of independence. The frequency and scope of ICT audits shall be commensurate to the ICT risk profile of the financial entity.

10. Based on the conclusions of the internal audit review, financial entities shall establish a formal follow-up process, including procedures for the timely verification and remediation of critical ICT audit findings (Article 6(7) of DORA).

11. Small and non-interconnected (Class 3) investment firms are reminded that they are subject to a simplified ICT risk management framework in accordance with the principle of proportionality as indicated in TITLE III of the Commission Delegated Regulation (EU) 2024/1774.

D. Information in CySEC Portal

12. Regulated Entities, other than microenterprises, are required to designate in the CySEC Portal the ICT auditor responsible for the internal audit of the ICT risk management framework, as per Article 6(6) of DORA.

13. The ICT auditor shall be designated under the Auditors section in the CySEC Portal, by completing the relevant details of the legal entity or natural person and selecting the option "Is ICT" (shown below):

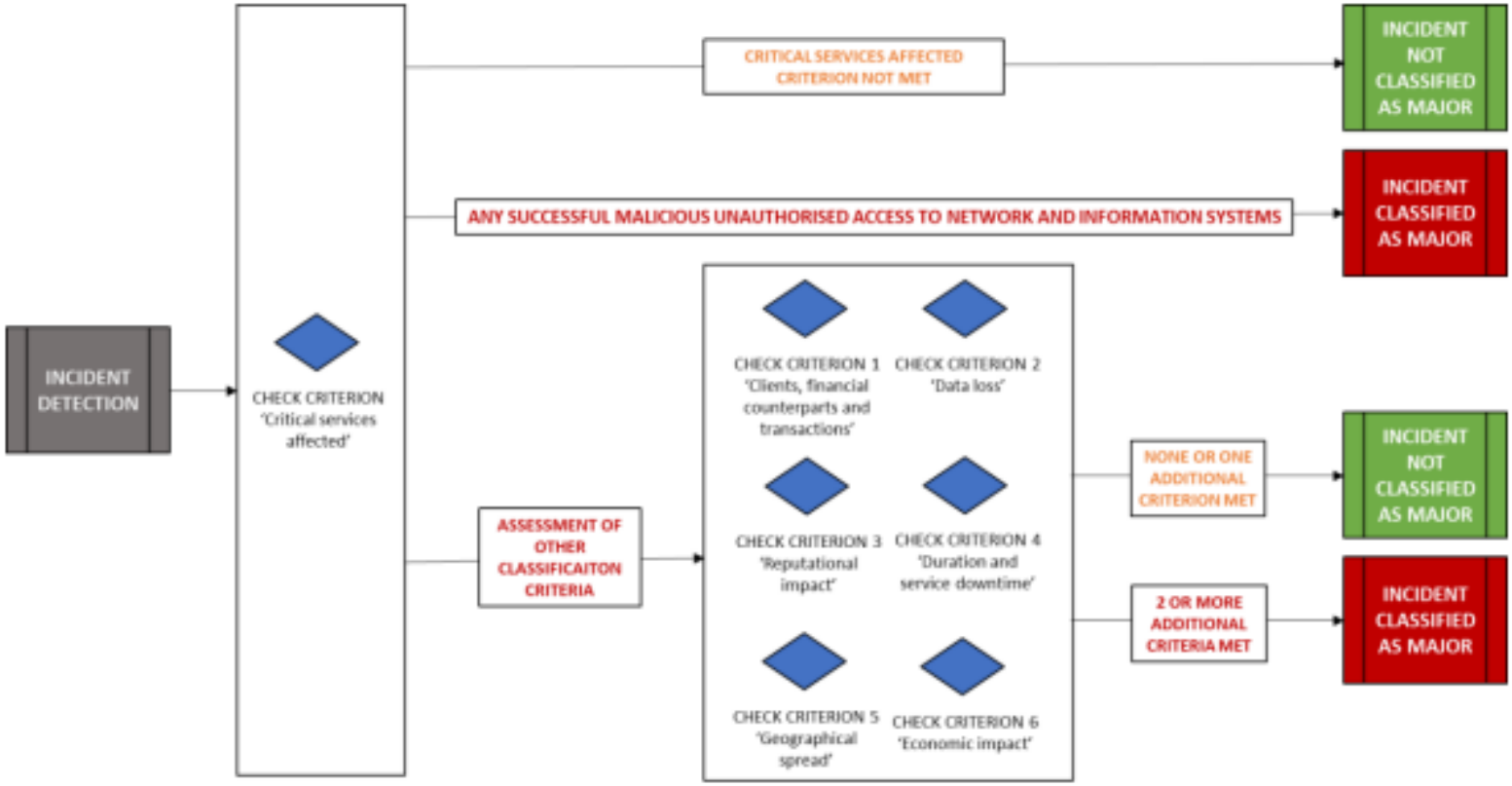
14. Regulated Entities are further required to designate in the CySEC Portal under the Personnel section, the person responsible for the control function entrusted with the management and oversight of ICT risk, as per Article 6(4) of DORA.

For any queries, Regulated Entities may contact CySEC in writing via email at prudential@cysec.gov.cy .

Yours sincerely,

Dr George Theocharides
Chairman
Cyprus Securities and Exchange Commission

Figure 1: Approach for classifying major incidents under DORA



Διαγόρου 19, 1097 Λευκωσία, Κύπρος / Τ.Θ. 24996, 1306 Λευκωσία, Κύπρος
Τηλ: (+357) 22506600, Φαξ: (+357) 22506700
Email: info@cysec.gov.cy, Web: www.cysec.gov.cy

19 Diagorou, CY-1097 Nicosia, Cyprus / P.O. Box 24996, CY-1306 Nicosia, Cyprus
Tel: (+357) 22506600, Fax: (+357) 22506700
Email: info@cysec.gov.cy, Web: www.cysec.gov.cy