EUROPEAN CENTRAL BANK

EUROSYSTEM

**ECB-PUBLIC**

# COMMENTS ON THE DRAFT "CYBER RESILIENCE OVERSIGHT EXPECTATIONS FOR FINANCIAL MARKET INFRASTRUCTURES"

| | | | |
|---|---|---|---|
| **Name of the originator (i.e. name of the company or association)** | Blue Media S.A. | ISO code of the country of the originator | PL |

**Comments on the draft Cyber Resilience Oversight Expectations for Financial Market Infrastructures**

| Issue | Comment | Reasoning |
|---|---|---|
| Resumption within 2 hours | Amendment | Resumption within two hours (i.e. 2-hour RTO) - RTO (recovery time objective i.e. time required to recover service/application from crash/disaster) should be result of a compromise/negotiations between service provider and service recipient and/or result of Business Impact Analysis process, where costs, abilities, requirements are analyzed and compromise is set. For some service/application 2hour RTO is unacceptably long, for others it can be unnecessarily too short - it should be always dependent on context and real requirements of service recipient and abilities of service provider |
| Testing Red teams | Amendment | Requirement for red team tests should be implemented over longer period of time (there should be some transition period for making it obligatory). Smaller financial companies don't have to many security personnel and they may not be able to perform read team or penetration tests internally and using external companies may pose some risks to financial data they process. It would be good to set some expectations for companies that perform FMI security audits and tests - it could be either certifications or list of requirements to allow them to run FMI audits/test. Local financial authorities should also maintain a list of companies that are trustful and capable of running such audits/tests etc. |