MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

5 September 2023

Update and Benchmarking Exercise on Regulation (EU) 2022/2554 on Digital Operational Resilience

1. Update

This Circular is an update to Circular titled Regulation (EU) 2022/2554 and Amending Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector published on the EU Official Journal published by the Authority in January 2023. As detailed by the latter Circular, Regulation (EU) 2022/2554 ("the Regulation") shall apply from 17 January 2025.

The Regulation places several requirements on the financial entities within scope, in the areas of ICT risk management; ICT-related incident management, classification and reporting; digital operational resilience testing (including advanced testing based on Threat-Led Penetration Testing); managing of ICT third-party risk (including an Oversight Framework of critical ICT third-party service providers); and voluntary information-sharing arrangements. The Regulation will also be supplemented by Regulatory/Implementing Technical Standards, (the "Technical Standards") being drafted by the European Supervisory Authorities (the "ESAs") through the Joint Committee. Delivery deadlines for these Technical Standards have been detailed in Annex 1 of the above-mentioned Circular. The Authority has also issued a Circular informing stakeholders of the ESAs Joint Committee Public Consultation on the First Set of Technical Standards under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector.

The obligations on financial entities in terms of the ICT-related areas outlined above, will change when compared to the obligations emanating from ICT-related provisions within the current applicable Acts, Regulations, Rules and/or sector-specific Guidelines.

The Authority is reaching out to the industry using various means, including: written communications, such as circulars; a periodic DORA Videocast; Frequently Asked Questions (which can be accessed by clicking on the Legislation sub-button); public consultations (e.g. Consultation Document on the Adoption of the TIBER-EU Framework in Malta); and events, such as webinars. Authorised Persons are expected to keep abreast with ongoing updates, particularly with the following upcoming developments:

- Public Consultation on the national implementation of the Regulation and the national transposition of the Amending Directive, planned to be issued by the Authority in

Quarter 4, 2023. Interested stakeholders will be invited to share their views with the Authority.

- The ESAs Joint Committee public consultation on the second set of Technical Standards. Interested stakeholders will be invited to share their views with the ESAs.

2. Benchmarking Exercise

The Authority expects the management bodies of financial entities within scope of the Regulation to ascertain that their financial entity is on track in its preparations to ensure compliance with the Regulation by its date of applicability (17 January 2025). The Authority expects that, as a minimum and as at the date of this Circular, financial entities:

1. have duly informed the management body of the Regulation;
2. have duly informed key function holders of the Regulation, including representatives from the Three Lines of Defence.
3. are keeping themselves abreast with any updates in relation to the development of the Technical Standards;
4. are duly aware of new reporting requirements and/or changes to existing reporting requirements, as specified by the Regulation;
5. have duly discussed and planned for possible new compliance costs arising from the Regulation;
6. have carried out a gap analysis between its present relevant strategies, policies, procedures, plans, systems, tools and the requirements of the Regulation;
7. have formally adopted a transition plan towards compliance with the Regulation that has been approved by the management body and duly communicated accordingly;
8. if applicable, have engaged in discussions with their external auditors and/or consultants regarding the Regulation;
9. if applicable, have engaged in discussions with their ICT Third Party Service Providers regarding the Regulation.

Authorised Persons may request further information or provide any feedback by sending an e-mail to the Supervisory ICT Risk and Cybersecurity function within the MFSA on sirc@mfsa.mt.