25 March 2024

Supervisory ICT Risk and Cybersecurity
Tel: (+356) 21441155

The Board of Directors

Dear Members of the Board/Chief Executive Officer ('CEO'),

Re: The Authority's Minimum Expectations in Relation to Financial Entities' Preparedness to Regulation (EU) 2022/2554 on Digital Operational Resilience

Background

On 16 January 2023, Regulation (EU) 2022/2554 (the 'DORA Regulation') and Amending Directive (EU) 2022/2556 (the 'DORA Amending Directive') came into force. The DORA Regulation and the DORA Amending Directive shall apply from 17 January 2025. This development has been communicated by the Malta Financial Services Authority (the 'MFSA', or the 'Authority') through a Circular published on 4 January 2023 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'.

The Authority has been engaging with Financial Entities within scope of the DORA Regulation (please refer to Article 2(1) of the DORA Regulation) on an on-going basis with a view to contribute towards their transition towards compliance with the DORA Regulation by its date of applicability (17 January 2025).

As established by the MFSA 2024 Supervisory Priorities document, the Supervisory ICT Risk and Cybersecurity ('SIRC') function will be focusing on ***Sufficient DORA Preparedness***, one out of four outcomes, that it intends to achieve through its supervision in 2024. More information on **Outcome-Based Supervision** can be found within the referenced document.

The Authority's 2023 Minimum Expectations *vis-à-vis* Sufficient DORA Preparedness

In 2023 the Authority sent a letter titled '*Financial Entity's Compliance with Regulation (EU) 2022/2554 on Digital Operational Resilience*', addressed to several Boards of Directors of Financial Entities within scope of the DORA Regulation, following a risk-based approach. This letter outlined a number of expectations (the '2023 Minimum Expectations') which were also communicated to the industry via Circular titled Update and Benchmarking Exercise on Regulation (EU) 2022/2554 on Digital Operational Resilience, published by the Authority in September 2023, listed in the next page.

Expectation 1: Financial Entities have duly informed the management body of the DORA Regulation.

Expectation 2: Financial Entities have duly informed key function holders of the DORA Regulation, including representatives from the Three Lines of Defence.

Expectation 3: Financial Entities are keeping themselves abreast with any updates in relation to the development of the Technical Standards.

Expectation 4: Financial Entities are duly aware of new reporting requirements and/or changes to existing reporting requirements, as specified by the DORA Regulation.

Expectation 5: Financial Entities have duly discussed and planned for possible new compliance costs arising from the DORA Regulation.

Expectation 6: Financial Entities have carried out a gap analysis between its present relevant strategies, policies, procedures, plans, systems, tools and the requirements of the DORA Regulation.

Expectation 7: Financial Entities have formally adopted a transition plan towards compliance with the DORA Regulation that has been approved by the management body and duly communicated accordingly.

Expectation 8: Financial Entities, if applicable, have engaged in discussions with their external auditors and/or consultants regarding the DORA Regulation.

Expectation 9: Financial Entities, if applicable, have engaged in discussions with their ICT Third Party Service Providers regarding the DORA Regulation.

The feedback received by the Authority on the 2023 Minimum Expectations suggests that there is a high-level of management body and key function holder **awareness** in relation to the DORA Regulation, its Technical Standards and new reporting requirements. The **concrete** aspect of the 2023 Minimum Expectations, such as planning for new compliance costs, the execution of a gap analysis and the adoption of a transition plan, however, is still largely in progress. Figure 1 in the next page portrays a visual illustration of the progress related to the 2023 Minimum Expectations, ordered by the level of progress (the expectation at the bottom being the expectation where the most progress has been reported and the topmost one where the least progress has been reported). As the date of applicability of the DORA Regulation approaches, the Authority expects tangible progress against the 2023 Minimum Expectations.

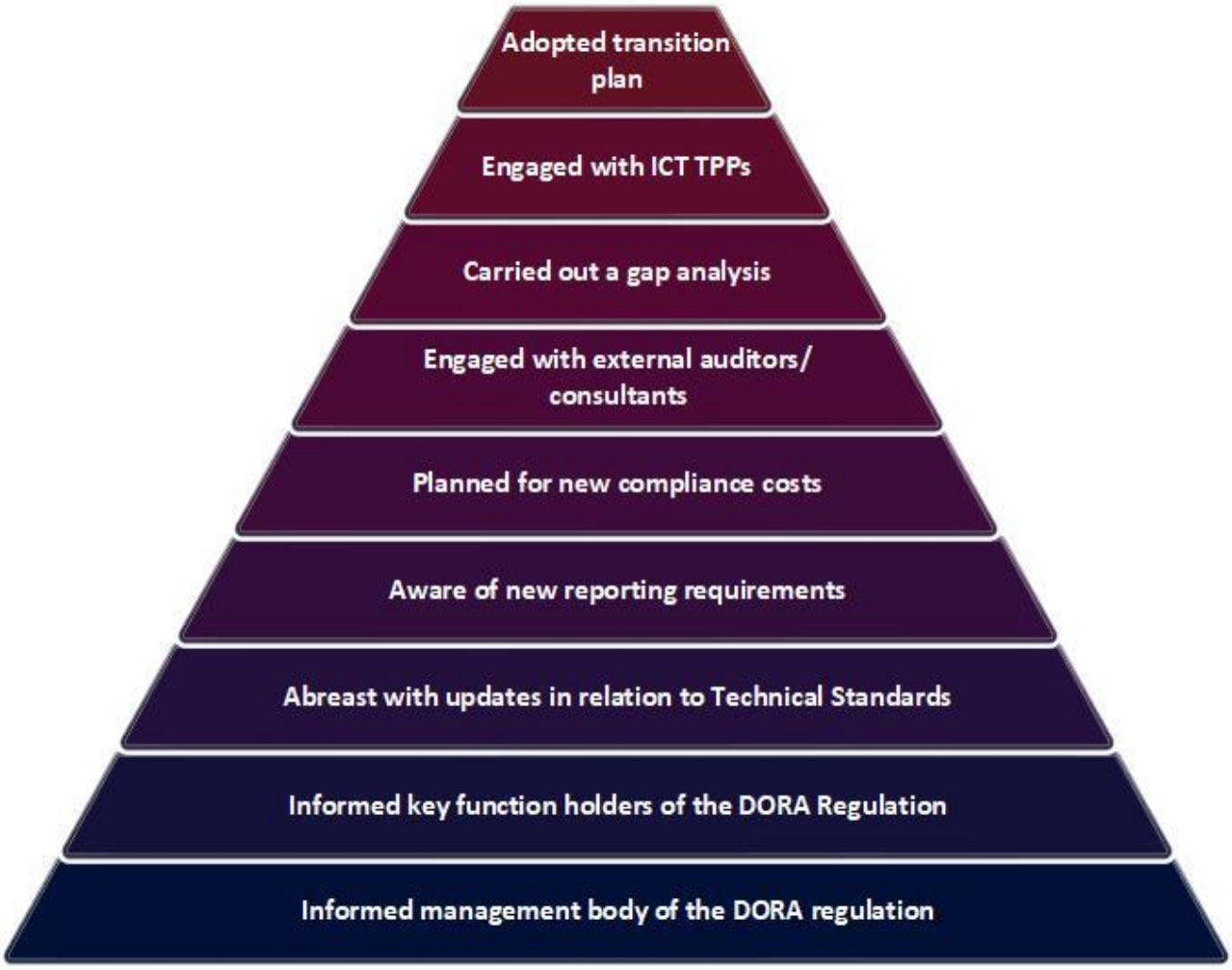

Figure 1: Progress on the 2023 Minimum Expectations

(+356) 2144 1155
info@mfsa.mt
www.mfsa.mt

Malta Financial Services Authority
Triq l-Imdina, Zone 1
Central Business District, Birkirkara, CBD 1010, Malta

The Authority's 2024 Minimum Expectations *vis-à-vis* Sufficient DORA Preparedness

This year the Authority expects a more advanced level of DORA preparedness and the following expectations 10 to 17 are the minimum expectations for 2024 (the '2024 Minimum Expectations').

Expectation 10: Financial Entities have taken steps towards developing a digital operational resilience strategy, as referred to in Article 6(8) of the DORA Regulation.

Expectation 11: Financial Entities have taken steps towards developing a DORA compliant ICT Risk Management Framework, in accordance with Chapter II of the DORA Regulation and have taken into consideration the Regulatory Technical Standard referred to in Articles 15 and 16(3) of the DORA Regulation.

Expectation 12: Financial Entities have taken steps towards developing an ICT-related incident management process as referred to in Article 17 of the DORA Regulation, and have taken into consideration the relevant provisions emanating from the Regulatory Technical Standard referred to in Articles 15 and 16(3) of the DORA Regulation.

Expectation 13: Financial Entities have taken steps towards ensuring that the classification and reporting of Major ICT-Related Incidents and the voluntary notification of Significant Cyber Threats are in accordance with the relevant Regulatory and Implementing Technical Standards supplementing Chapter III of the DORA Regulation.

Expectation 14: Financial Entities have taken steps towards developing a digital operational resilience testing programme, in accordance with Articles 24 and 25 of the DORA Regulation.

Expectation 15: Financial Entities have taken steps towards managing their ICT third-party risk including: if applicable, a strategy on ICT third-party risk as provided by Article 28(2) of the DORA Regulation; and a policy on the use of ICT services supporting critical or important functions taking into consideration the Regulatory Technical Standard referred to in Article 28(10).

Expectation 16: Financial Entities have taken steps towards developing a Register of Information ('RoI'), in accordance with Article 28(3) of the DORA Regulation and taking into consideration the Implementing Technical Standard referred to in Article 28(9).

Expectation 17: Financial Entities have taken steps towards aligning their current written contractual arrangements with ICT Third-Party Service Providers to the key contractual provisions specifically mentioned in Article 30 of the DORA Regulation.

The Approach towards Sufficient DORA Preparedness as a 2024 Supervisory Outcome

The Authority continues to expect management bodies to ensure that their respective Financial Entities are on track to ensure compliance with the DORA Regulation by its date of applicability. In 2024, Financial Entities are expected to address any gaps in meeting the 2023 Minimum Expectations, particularly regarding concrete action, as well as to meet the 2024 Minimum Expectations by taking **steps towards the development of strategies, frameworks, policies and procedures.** Figure 2 in the next page provides a visual illustration of this approach. The Authority will be engaging with your Financial Entity using any of the different supervisory tools available to it, such as within the context of a Supervisory Inspection, a Thematic Review, an ICT Risk Questionnaire, or a separate Dear CEO letter, to assess your Financial Entity's progress against the 2023 and 2024 Minimum Expectations.

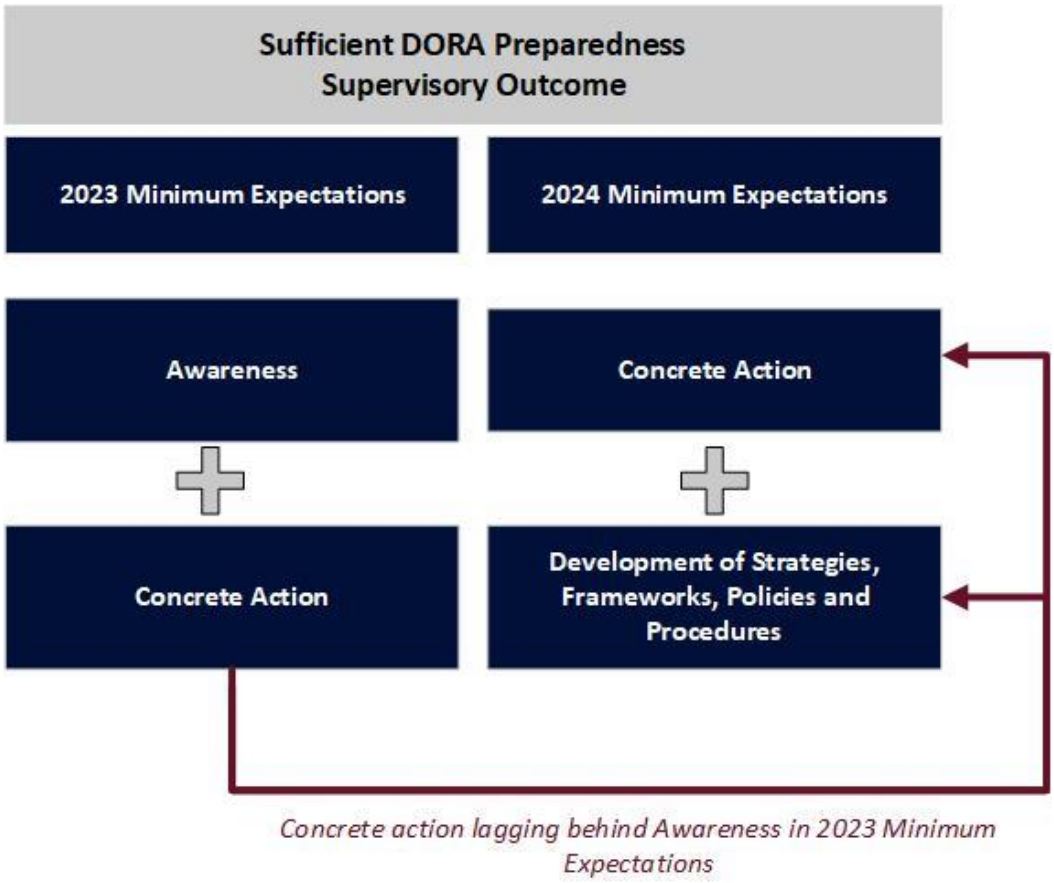

Figure 2: Sufficient DORA Preparedness as a Supervisory Outcome

Conclusion and Way Forward

Sufficient DORA Preparedness is one of the outcomes that the Authority intends to achieve through its supervision in 2024 as outlined in the MFSA 2024 Supervisory Priorities document. This letter provides the minimum expectations of the MFSA vis-à-vis the respective Financial Entities in this regard. The Authority will be separately engaging with your Financial Entity to gather information in relation to your progress against these expectations in due course.

Please be guided accordingly.

Should you have any queries in relation to the above, please do not hesitate to contact the Supervisory ICT Risk and Cybersecurity function on sirc@mfsa.mt.

Yours Sincerely,
Malta Financial Services Authority

Christopher Peter BUTTIGIEG (Signature)
Digitally signed by Christopher Peter BUTTIGIEG (Signature)
Date: 2024.03.22 10:15:33 +01'00'

Christopher P. Buttigieg
Chief Officer Supervision

Alan DECELIS (Signature)
Digitally signed by Alan DECELIS (Signature)
Date: 2024.03.22 09:06:25 +01'00'

Alan Decelis
Head – Supervisory ICT Risk and Cybersecurity

(+356) 2144 1155
info@mfsa.mt
www.mfsa.mt

Malta Financial Services Authority
Triq l-Imdina, Zone 1
Central Business District, Birkirkara, CBD 1010, Malta