MFSA MALTA FINANCIAL SERVICES AUTHORITY

Feedback Statement

Feedback Statement to Queries Raised by Consulted Stakeholders on Regulation (EU) 2022/2554 on Digital Operational Resilience (the 'DORA Regulation')

Date: 19 February 2024

Contents

1. Introduction

This Feedback Statement is a follow-up to the letter sent by the Malta Financial Services Authority ('MFSA', 'the Authority') on 5 September 2023 titled *Queries on Regulation (EU) 2022/2554 on digital operational resilience (the 'DORA Regulation')*. The letter was sent to Institutions and Associations in Malta, covering financial services sectors within scope of the DORA Regulation. The Authority would like to thank all the Associations and Institutions for the queries made.

The Authority has aggregated all the queries that it has received and is providing aggregate feedback, without prejudice to any applicable Acts, Regulations, Rules and/or sector-specific Guidelines, via this document. At the same time, some of the queries and their respective replies will also be included to the Frequently Asked Questions ('FAQs') available online on the MFSA website (Our Work > Supervisory ICT Risk and Cybersecurity > Legislation).

The Authority would like to take this opportunity to provide some general updates on the DORA Regulation and its national implementation. As informed by the Authority via 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, the DORA Regulation is supplemented by a series of, inter alia, Technical Standards with delivery deadlines of January 2024 (hereinafter referred to as 'the first set of Technical Standards) and July 2024 ('the second set of Technical Standards').

As informed via Circular titled 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 European Supervisory Authorities ('ESAs') have carried out a public consultation on the first set of Technical Standards. The public consultation is now closed, and the first set of Technical Standards has been submitted to the European Commission, as informed via Circular titled First Set of Technical Standards under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector Submitted to the European Commission.

The second set of Technical Standards is currently open for public consultation until 4 March 2024, as informed via Circular titled ESAs Joint Committee Public Consultation on the Second Set of Technical Standards under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector.

Lastly, in relation to the national implementation of the DORA Regulation, the Authority has released a Consultation Document on the National Implementation of Regulation (EU) 2022/2554 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector. The Authority has also released a Feedback Statement on the Adoption of the TIBER-EU Framework in Malta.

2.1 General Queries

Timeline for Compliance

Feedback Received

Stakeholders asked for further clarifications on the Authority's expectations in relation to financial entities' compliance with the DORA Regulation by its official date of applicability in January 2025.

Authority's Reply

For the avoidance of doubt, it should be noted that the date of applicability of the DORA Regulation cannot be changed by the Authority because it is a direct legal requirement emanating from the DORA Regulation itself. The Authority acknowledges that financial entities might face certain challenges to transition towards compliance with the DORA Regulation by its date of applicability, especially when considering the delivery deadlines of the Technical Standards. The Authority will indeed take this into consideration when evaluating Authorised Persons' compliance with the DORA Regulation.

2.2 Queries Relating to Chapter II

Guidance on the Identification of Critical and Important Functions

Feedback Received

Stakeholders asked for general guidance on how financial entities can go about the identification of their critical and important functions, according to the DORA Regulation.

Authority's Reply

It should be noted that guidance on the identification of critical and important functions is provided by Article 3(22) of the DORA Regulation:

> *"'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law;"*

Therefore, financial entities should carry out such identification in line with the above-mentioned definition.

Guidance on the Digital Operational Resilience Strategy

Feedback Received

Stakeholders asked for guidance on the Authority's expectations in relation to the digital operational resilience strategy, as referred to in Article 6(8) of the DORA Regulation. Stakeholders questioned whether the Authority will establish derogations vis-à-vis the holistic ICT multi-vendor strategy, to be included under the financial entities' digital operational resilience strategy, pursuant to Article 6(9) of the DORA Regulation.

Authority's Reply

Without prejudice, the digital operational resilience strategy established by the DORA Regulation can be understood as a strategy adopted by the financial entity which sets out how the ICT risk management framework is implemented in the financial entity, in line with Article 6(8) of the DORA Regulation. Article 6(8) points (a) to (h) further specify the expectations in relation to the digital operational resilience strategy.

In relation to the ICT multi-vendor strategy, Article 6(9) of the DORA Regulation provides:

> *"Financial entities may, in the context of the digital operational resilience strategy referred to in paragraph 8, define a holistic ICT multi-vendor strategy, at group or entity level, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers."*

Therefore, financial entities may choose to establish a holistic ICT multi-vendor strategy in the context of their digital operational resilience strategy.

Contents of the Reporting of the Review of the ICT Risk Management Framework

Feedback Received

Stakeholders requested further clarity on the contents of the report on the review of the ICT risk management framework, as referred to in Article 6(5) of the DORA Regulation.

Authority's Reply

Pursuant to Article 15(1)(g) of the DORA Regulation, there shall be a Technical Standard that further supplements the contents of the report on the review of the ICT risk management framework. More information on the contents of such report can be found in the Final Report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554, released by the ESAs.

2.3 Queries Relating to Chapter III

Reporting of Major ICT-related Incidents and Voluntary Notification of Significant Cyber Threats

Feedback Received

Stakeholders questioned whether the Authority will be the designated recipient of major ICT-related incidents and significant cyber threats and whether financial entities will also be required to send the reports and notifications to the designated national Computer and Security Incident Response Team (hereinafter referred to as the 'National CSIRT') under Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (hereinafter referred to as 'NIS2'). Stakeholders also required a clarification on the interplay between the incident reporting mechanism under the DORA Regulation, and the reporting mechanism established under Directive 2015/2366/EU (hereinafter referred to as 'Payment Services Directive 2' or 'PSD2').

From a practical perspective, stakeholders have questioned whether the Authority will establish a new channel for the reporting of major ICT-related incidents and the voluntary notification of significant cyber threats.

Lastly, stakeholders asked for further information on the Authority's expectations *vis-à-vis* the reporting of ICT-related Incidents by financial entities which are not under the scope of the DORA Regulation.

Authority's Reply

As outlined in the Consultation Document on the National Implementation of Regulation (EU) 2022/2554 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector, it is proposed that the Authority shall be the recipient of any major ICT-related incident reports and any voluntary notification of significant cyber threats, in terms of Article 19 of the DORA Regulation. It is also proposed that the Authority may transmit to the national CSIRT any major ICT-related incident reports and any voluntary notifications of significant cyber threats. In other

words, financial entities would report both major ICT-related incident reports and/or voluntarily notify significant cyber threats to the Authority. Any onward transmission of reports and/or notifications to the National CSIRT, where applicable, would be carried out by the Authority itself.

Regarding PSD2, as pointed out by one of the Authority's FAQs and episode 7 of our videocast titled The Interplay Between Different Incident Reporting Mechanisms and DORA, the Authority notes that DORA Amending Directive (EU) 2022/2556 amends PSD2. According to DORA recital (23):

> *"To reduce the administrative burden and potentially duplicative reporting obligations for certain financial entities, the requirement for the incident reporting pursuant to Directive (EU) 2015/2366 of the European Parliament and of the Council should cease to apply to payment service providers that fall within the scope of this Regulation. Consequently, credit institutions, e-money institutions, payment institutions and account information service providers, as referred to in Article 33(1) of that Directive, should, from the date of application of this Regulation, report pursuant to this Regulation, all operational or security payment-related incidents which have been previously reported pursuant to that Directive, irrespective of whether such incidents are ICT-related."*

In relation to reporting channels for both major ICT-related incident reports and notifications of significant cyber threats, as outlined by episode 5 of our videocast titled ICT-Related Incidents under DORA**,** the Authority is currently working on aligning its current incident reporting mechanism to the requirements of the DORA Regulation. The Authority will keep stakeholders and Authorised Persons informed of any developments in relation to this via the appropriate channels.

The Authority will be communicating its incident reporting expectations applicable to financial entities which are not in scope of the DORA Regulation at a later stage.

Estimates of Aggregated Annual Costs/Losses Caused by Major ICT-related Incidents

Feedback Received

Stakeholders questioned whether the Authority will request financial entities to provide an estimate of aggregated annual costs/losses caused by major ICT-related incidents, as provided by Article 11(10) of the DORA Regulation, in January 2025.

Authority's Reply

In relation to timeline, paragraph (5) of the Consultation Paper on Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents released by the ESAs currently provides the following:

> *"Financial entities should estimate the aggregate annual costs and losses of major ICT-related incidents by aggregating the costs and losses for major ICT-related incidents that fall within the reference period. The reference period should be the completed accounting year for which the competent authority requested the estimation. Financial entities should not include costs and losses related to those incidents that fall before or after that reference period."*

The above-mentioned Guidelines are currently in draft format and therefore subject to change, following feedback gathered from the public consultation.

Without prejudice, the Authority plans to request an estimate of aggregated annual costs/losses caused by major ICT-related incidents, in accordance with the above-mentioned guidelines, for those financial entities that report a major ICT-related incident.

2.4 Queries Related to Chapter V

Register of Information

Feedback Received

Stakeholders questioned the Authority's expectations in relation to the Register of Information, to be kept by financial entities, as referred to in Article 28(3) of the DORA Regulation. This includes whether financial entities should include intra-group ICT Third Party Service Providers ('ICT TPPs') within their Register. In addition, stakeholders requested a clarification on when they will need to first report the Register.

Authority's Reply

As mandated by Article 28(9) of the DORA Regulation, there shall be a Technical Standard that further supplements the contents of the Register of Information. The content of the Register of Information can be found in the Final Report on Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT

services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554.

In this respect, financial entities should include intra-group ICT TPPs within their Register of Information, as further clarified by recital (8) of the above-mentioned proposed Technical Standard:

> *"In line with Article 30(1) of the Regulation (EU) 2022/2554, in order to receive any type of ICT services from an ICT third-party service provider, including from ICT intragroup service providers, financial entities negotiate a written contract with the ICT third-party service provider. In case of groups, ICT intra-group service providers may arrange a contract with ICT third-party providers external to the group to provide ICT services to one or more financial entities of the group. In order to capture the full ICT service supply chain under such practice, financial entities maintaining the register of information at entity level report both information on the contractual arrangement with their ICT intra-group service provider and on the arrangement stipulated by the ICT intra-group service provider and the ICT third-party providers external to the group as sub-contractors. In order to manage this and other similar cases, the register of information at sub-consolidated and consolidated level includes a template allowing the reconciliation between the intra-group contracts and the contracts with ICT third-party service providers external to the group."*

Without prejudice, the Authority can request the Register of Information as of 17 January 2025, in line with the date of applicability of the DORA Regulation. Therefore, financial entities should ensure that their Registers of Information are duly in place by this date. This specific point has been previously addressed by the ESAs in the Consultation Paper On Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554 (specifically available under *section 5 on draft cost-benefit analysis/impact assessment, Policy Issue 10: Date of Application*).

2.5 Queries Relating to Chapter VI

Digital Operational Resilience Testing

Feedback Received

Stakeholders requested a clarification on whether the digital operational resilience testing programme established in Article 24 of the DORA Regulation will apply to the financial entities referred to in Article 16 of that same regulation.

Authority's Reply

The digital operational resilience testing programme established in Article 24 of the DORA Regulation does not apply to financial entities which qualify as, or are subject to the simplified ICT risk management framework under the DORA Regulation, as further specified in recital (43) of the DORA Regulation:

> *"Similarly, financial entities which qualify as microenterprises or are subject to the simplified ICT risk management framework under this Regulation should not be required to […] to establish a comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework provided for in this Regulation […]"*

However, it should be noted that there are draft provisions relating to ICT security testing in the simplified ICT risk management framework in the Final Report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554, released by the ESAs.

Selection of Financial Entities and Testing Frequency for Advanced Testing Through Threat-Led Penetration Testing ('TLPT')

Feedback Received

Stakeholders questioned which financial entities within scope of the DORA Regulation will be selected to undergo TLPT and when this information will be made available to the relevant financial entities. In addition, stakeholders have also questioned whether – and, if so, when – the Authority will inform financial entities required to perform TLPT on the frequency of the tests, as set out in Article 26(1) of the DORA Regulation.

Authority's Reply

The criteria used for the purpose of identifying and assessing which financial entities will be subject to TLPT is, as mandated by Article 26(11) of the DORA Regulation, to be technically supplemented by a Technical Standard. The proposed identification and assessment criteria can be found under the Consultation Paper on Draft Regulatory Technical Standards specifying elements related to threat led penetration tests. This Technical Standard is currently in draft format and is subject to change, following feedback gathered from the public consultation. Once the text of the above-mentioned Technical Standard is final, the financial entities meeting the criteria for TLPT selection will be duly contacted by the Authority via the appropriate channels in sufficient time before they are subjected to a test.

In relation to the frequency of the tests, Article 26(1) of the DORA Regulation provides:

> *"Financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, which are identified in accordance with paragraph 8, third subparagraph of this Article, shall carry out at least every 3 years advanced testing by means of TLPT. Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity to reduce or increase this frequency."*

Without prejudice, whilst the Authority plans to be guided primarily by a three-year frequency, the Authority may, where necessary, request a financial entity to reduce or increase this frequency as provided by Article 26(1) during the course of the DORA applicability.

Expectations vis-à-vis Evidence of TLPT Testing in January 2025

Feedback Received

Stakeholders asked whether the Authority expects financial entities to provide evidence that TLPT tests have been carried out in accordance with the DORA Regulation in January 2025.

Authority's Reply

The DORA Regulation is applicable from 17 January 2025. Therefore, requesting evidence of completion of a TLPT as soon as the DORA Regulation becomes applicable, is highly unlikely, when considering that such tests can spread over an extended period of time.

As previously stated, without prejudice, financial entities meeting the criteria for TLPT selection will be duly contacted by the Authority via the appropriate channels in sufficient time before they are subjected to a test.

More information on TLPT can be found within the Consultation Paper on Draft Regulatory Technical Standards specifying elements related to threat led penetration tests. This Technical Standard is currently in draft format and is subject to change, following feedback gathered from the public consultation.

Status Update and Competent Authority for TLPT

Feedback Received

Stakeholders have asked for a status update to the Consultation Document on the Adoption of the TIBER-EU Framework in Malta, in addition to asking for a clarification on what authority/authorities is/are to be designated as responsible for TLPT-related matters at a national level, pursuant to Article 26(9) and (10) of the DORA Regulation.

Authority's Reply

The Authority has recently published a Feedback Statement on the Adoption of the TIBER-EU Framework in Malta. In relation to the authority responsible for TLPT, stakeholders are invited to refer to the Consultation Document on the National Implementation of Regulation (EU) 2022/2554 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector.

3. Contact

Authorised Persons and interested stakeholders may request further information by sending an email to the Supervisory ICT Risk and Cybersecurity function on sirc@mfsa.mt.