MFSA MALTA FINANCIAL SERVICES AUTHORITY

THE NATURE AND ART OF FINANCIAL SUPERVISION VOLUME XI

SUPERVISORY ICT RISK AND CYBERSECURITY

03 September 2024

Contents

Table of Abbreviations

CREs	Cyber Resilience Exercises
CTPP	Critical ICT Third-Party Provider
DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554)
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ESA	European Supervisory Authority
ESFS	European System for Financial Supervision
ESMA	European Securities and Markets Authority
ESRB	European Systemic Risk Board
EU	European Union
EU-SCICF	Pan-European Systemic Cyber Incident Coordination Framework
FAQs	Frequently Asked Questions
ICT	Information and Communications Technology
ICT TPP	ICT Third-Party Provider
NCSC	National Cybersecurity Steering Committee
RoI	Register of Information
SIRC	Supervisory ICT Risk and Cybersecurity (Function)
SITO	Systemic Impact Tolerance Objective
SMEs	Micro, Small and Medium-sized Enterprises
SREP	Supervisory Review and Evaluation Process
TIBER	Threat Intelligence-based Ethnical Red Teaming
TLPT	Threat-Led Penetration Testing

Introduction

With the increase of digital processes, tools, and the economy itself, the financial services sector has been increasingly relying on ICT. As a result, Financial Entities have increased their exposure to operational risk, more specifically to ICT risk. Against this backdrop, ICT, digital operational resilience, digital transformation and the DORA Regulation have been picked as key and strategic priorities of the ESAs[1] . Outside of the remit of the ESFS, the Basel Committee has also set the digitalisation of finance as part of the Basel Committee work programme and strategic priorities for 2023/24[2].

As the management of ICT and cyber risk has become an integral part of any supervisory toolkit, the SIRC Function was established in early 2020 with the aim of carrying out ICT and cyber-related supervision and to contribute towards digital operational resilience within the financial services sector. In order to do so, the SIRC Function works hand-in-hand with other supervisory functions.

Since its establishment, the SIRC Function achieved an enhanced level of maturity and this has been reflected in its achievements, as outlined throughout this publication. More specifically, this publication outlines how the Function has evolved in line with major relevant regulatory developments and how it aims to continue to contribute towards greater digital operational resilience and cyber-maturity in the Maltese financial sector. This publication also elaborates further on the SIRC Function's supervisory focus areas for 2024.

[1] See EBA's 2024 Work Programme, ESMA's 2024 Work Programme and EIOPA's Final Single Programming Document 2024-2026.

[2] Basel Committee work programme and strategic priorities for 2023/24.

Our Supervisory Approach

Within the previous publication of The Nature and Art of Financial Supervision Volume III in 2021, the SIRC Function's supervisory approach was based on a complex and fragmented regulatory framework, consisting of Payment Services Directive 2 ((EU) 2015/2366), Capital Requirements Directive (2013/36/EU), Capital Requirements Regulation ((EU) No 648/2012), Markets in Financial Instruments Directive II (2014/65/EU), European Market Infrastructure Regulation ((EU) No 648/2012), Solvency II Directive (2009/138/EC), Undertakings for Collective Investment in Transferable Securities Directive (2009/65/EC), the Alternative Investment Fund Managers Directive (2011/61/EU), Institutions for Occupational Retirement Provision Directive ((EU) 2016/2341), Central Securities Depositories Regulation ((EU) No 909/2014) and, where applicable, their national transposition. Moreover, on a more sectoral level, the Function's supervisory approach is also based on the requirements set out in the ESAs' and the MFSA's Guidelines, (hereafter collectively referred to as the 'Applicable Guidelines'), *inter alia*:

- EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04);
- EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02);
- EIOPA Guidelines on ICT Security and Governance (EIOPA-BoS-20/600);
- EIOPA Guidelines on Outsourcing to Cloud Service Providers (EIOPA-BoS-20-002);
- ESMA Guidelines on Outsourcing to Cloud Service Providers (ESMA50-157-2403); and
- The Authority's Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements (hereinafter referred to as the 'Guidance Document').

The above-mentioned Applicable Guidelines have been cross-referenced in the Authority's sectoral rulebooks. Therefore, as applicable, Authorised Persons within scope of these Rulebooks, are expected to comply with the ESAs' Guidelines and the

Guidance Document to the extent set out in the Rules. A complete list of such cross-references has been made available by the Authority via the document titled Cross-references to the Guidance Document on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements and applicable ESAs Guidelines (as of May 2023).

As outlined in the 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 has now come into effect. This Regulation will harmonize and streamline the requirements set out in the above listed regulatory framework. In line with this, the SIRC Function's supervisory approach has been evolving as to align itself to the requirements and expectations set out in the DORA Regulation.

The SIRC Function's efforts towards achieving alignment with the DORA Regulation continued with clearer contours, as the Function gained more clarity on the Regulation itself and its interaction with other cybersecurity-related legal instruments, for instance, as outlined by circular titled Directives (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity and (EU) 2022/2557 on the Resilience of Critical Entities, published by the Authority in January 2023.

In a proactive manner, the SIRC Function carried out internal changes with the aim to start its long-term alignment process with the DORA Regulation through internal restructuring and the adoption of several processes. These processes are, *inter alia*: Legislation and Policy Management; ICT-related Incident Reporting and Management; Significant Cyber Threat Notification and Management; Cyber Resilience Exercises; Coordination Frameworks; ICT Risk Questionnaires and Horizontal Analyses; Supporting Authorisations; Information-Sharing Arrangements; On-going Supervision; ICT Third-Party Risk; TLPT; and Outreach.

2024 Supervisory Priorities and Outcome-Based Supervision

The SIRC Function's supervisory approach and processes are aligned with the Authority's many efforts *vis-à-vis* supervision. More specifically, the Authority's 2023 Strategic Statement identified a series of high-level areas upon which the Authority intends to work until 2025. The work carried out by the SIRC Function contributes towards Strategic Priority 10 and, more broadly, Strategic Priority 22 within the context of the national implementation of the DORA Regulation.

As in previous years, in 2024 the Authority released the MFSA Supervision Priorities 2024 specifying the main supervisory and regulatory priorities, in line with the strategic priorities outlined by the Authority's 2023 Strategic Statement. Based on results derived from its supervisory engagements, the SIRC Function established four priorities (refer to Figure 2) as follows: (1) sufficient DORA preparedness; (2) implementation of strong risk management and compliance functions; (3) adequate incident management processes; and (4) satisfactory status of ICT TPPs.

In 2024, the SIRC Function adopted the Authority's pilot project that introduces, for the first time in the Maltese financial services supervision context, an Outcomes-based Supervisory approach as defined in the 2024 MFSA Supervision Priorities.

> *"Outcome-based supervision is the focus on the intended results from supervisory practices and deriving an efficient way to achieve them, to maintain the three goals of financial regulation: Consumer Protection, Financial Stability and Market Integrity."*[3]

Complementing its existing risk-based approach models, Outcomes-based Supervision will contribute amply to the Maltese financial services sector by introducing additional transparency measures, minimising ambiguity, strengthening data quality and data capacity, and most importantly, bringing to the fore measurable and effective tangible outcomes. Hence, whereas the risk-based approach models will continue to aid in the identification of Authorised Persons that will be in scope of a supervisory engagement, the Outcomes-based Supervisory approach will assist in the concise identification of the intended results of the supervisory engagement itself.

[3] MFSA Supervision Priorities 2024.

To this extent, Outcomes-based Supervision will be spread across a three-year cycle, where on the first year, the Authority will engage and assess its Authorised Persons, affording a lead time of another year thereafter to Authorised Persons as a remediation period, and on the third and final year, the Authority will re-engage and re-assess with the same Authorised Persons, using the same set of controls, to measure their implementation, impact, and effectiveness (Figure 1).

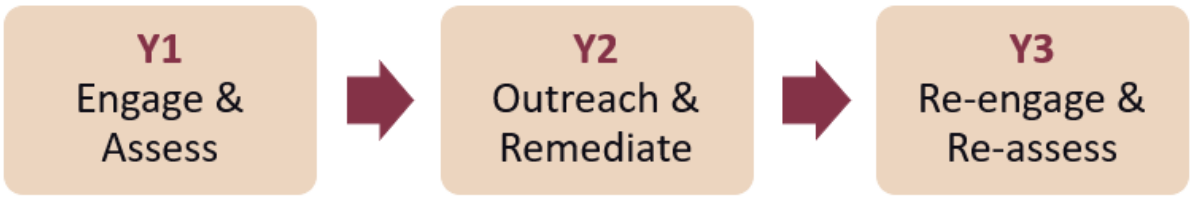

Figure 1: Outcome-Based Supervision

Through the Outcomes-based Supervisory approach, SIRC will be publishing, *a priori*, a list of Supervisory Outcomes upon which the controls under assessment for that year will be devised upon, where each control will be founded upon existing statutory provisions, predominantly the DORA Regulation and the MFSA Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements for those Authorised Persons who do not fall within scope of the DORA Regulation.

Additionally, each control will be risk-rated using a pre-defined list of determining factors and an accompanying risk scoring matrix. For example, whereas some controls will pose a major bearing on the overall outcome of a Supervisory Engagement, other controls will have less impact on the engagement as a whole. This is also because the law itself contemplates instances where the unavailability of a control is detrimental to Authorised Persons, whilst others pose a lesser risk.

The SIRC Function aligned its Supervisory Outcomes with the above-mentioned supervisory priorities, as detailed below:

1) **Sufficient DORA Preparedness:** the aim of this outcome is to engage with supervised entities on their preparations to comply with the DORA Regulation;
2) **Implementation of Strong Risk Management and Compliance Functions**: the aim of this outcome is to assess supervised entities' risk management and

compliance function (2nd line of defence) with a focus on ICT risk and cybersecurity;

3) **Adequate Incident Management Processes**: the aim of this outcome is to evaluate supervised entities' preparedness against cybersecurity risks that threaten confidentiality, integrity and availability of ICTs; and
4) **Satisfactory Status of ICT TPPs**: the aim of this outcome is to ensure, *inter alia*, the retention ICT outsourcing registers, conduct of risk assessments regarding risks stemming from ICT TPPs, the implementation of proportionate controls and the retention of satisfactory written contractual arrangements by Authorised Persons.

Figure 2: Supervision Priorities of the SIRC Function for 2024

More detail on the SIRC Function's 2024 Supervisory Priorities and its efforts towards outcome-based supervision can be found within the MFSA Supervision Priorities 2024 document under section titled '*SIRC – Outcome-Based Supervision*'.

Legislation and Policy Management

Since the publication of The Nature and Art of Financial Supervision Volume III in 2021 and the designation of the DORA Regulation as one of the Authority's 2022 cross-sectoral priorities, outlined in the MFSA Supervision Priorities 2022 document, the DORA Regulation has been published in the EU Official Journal and has come into force on 16 January 2023. The Regulation will be fully applicable as of 17 January 2025, following a two-year implementation period.

The DORA Regulation aims towards a more harmonized and comprehensive set of requirements for the digital operational resilience of the financial sector. As already mentioned, previous requirements were spread out across numerous Regulations, Directives and ESAs Guidelines, an unnecessary level complexity which hindered both the activities of Financial Entities across the Union and that of supervisors.

Against a backdrop of regulatory complexity in the area of digital operational resilience, the pandemic accelerated digital transformation and deeper reliance of the sector on ICT TPPs as a way of achieving economies of scale. Therefore, whilst the dynamics of the risk on digital operational resilience was changing, the complex regulatory landscape was incapable of providing a sufficiently comprehensive and cohesive framework.

The solution proposed was the creation of the DORA Regulation – a comprehensive and cohesive Regulation that sets requirements with an aim to increase Financial Entities' digital operational resilience. As outlined and detailed in 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, the DORA Regulation is to be supplemented by a number of technical standards with delivery deadlines of January 2024 and July 2024 .

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 have carried out a public consultation on the first set of technical standards. Subsequently, the ESAs have submitted this set of technical standards to the European Commission, as detailed in 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, released by the Authority in January 2024.

The second set of technical standards was 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. The second set of technical standards was subsequently complemented by an ESAs Joint Committee Public Consultation on the Harmonisation of Conditions Enabling the Conduct of the Oversight Activities under Article 41(1) Point © of Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, which has been released in April 2024. In July 2024, the ESAs submitted the second set of technical standards to the European Commission, as detailed via Circular titled Second Set of Technical Standards under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector Submitted to the European Commission.

From a legal perspective, the DORA Regulation introduces amendments to the following regulations: Credit Rating Agencies Regulation ((EC) No 1060/2009); European Market Infrastructure Regulation ((EU) No. 648/2012); Central Securities Depositories Regulation ((EU) No 909/2014); Market in Financial Instruments Regulation ((EU) 600/2014); and Benchmark Regulation ((EU) No 2016/1011).

The DORA Regulation is also accompanied by an Amending Directive, which amends the following directives: Collective Investment in Transferable Securities Directive ((EU) 2009/65/EC); Solvency II Directive (2009/138/EC); Alternative Investment Fund Managers Directive (2011/61/EU); Capital Requirements Directive (2013/36/EU); Bank Recovery and Resolution Directive (2014/59/EU); Markets in Financial

Instruments Directive II (2014/65/EU); Payment Services Directive II ((EU) 2015/2366); and Institutions for Occupational Retirement Provision II Directive ((EU) 2016/2341).

With a view to implement the DORA Regulation and to transpose the DORA Amending Directive locally, the Authority has published 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.

A corresponding Feedback Statement on the National Implementation of Regulation (EU) 2022/2556 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector has been made available by the Authority. Subsequently, for the purposes of implementing the DORA Regulation, Legal Notice 166 of 2024 titled *Malta Financial Services Authority Act (Digital Operational Resilience Act (DORA)) Regulations, 2024* was published in the Government Gazette. The Legal Notice can be found here.

The national implementation of the DORA Regulation contributes towards the Authority's Strategic Priority 10 and, more broadly, Strategic Priority 22, as outlined in the Authority's Strategic Statement published in 2023; in addition to contributing towards the achievement of the National Cybersecurity Strategy 2023-2026, as specifically outlined within the said strategy. Significant work in relation to the DORA Regulation has been carried out in the area of outreach. More information can be found under section titled '*Outreach*' in this Nature and Art document.

The Five Pillars of the DORA Regulation

The DORA Regulation is comprised of five main pillars, these are: ICT risk management; ICT-related incident management, classification and reporting; digital operational resilience testing; managing of ICT third party risk and a voluntary pillar on information-sharing arrangements (Figure 3).

Figure 3: The Five Pillars of the DORA Regulation

Under the ICT risk management pillar, Financial Entities are required to have robust governance arrangements, in addition to a risk management framework with strategies, policies, procedures, protocols and tools to adequately manage ICT risk. Selected Financial Entities under Article 16 benefit from a simplified ICT risk management framework.

Under the pillar of ICT-related incident management, classification and reporting, Financial Entities are required to have procedures and processes for monitoring, handling and following-up ICT-related incidents. Furthermore, Financial Entities will be responsible for classifying incidents and reporting those considered to be major to the Authority. Additionally, entities may, on a voluntary basis, notify significant cyber threats.

The third pillar relates to digital operational resilience testing**:** Financial Entities need to have in place a digital operational resilience testing programme as part of their ICT risk management framework. Selected Financial Entities will be required to undergo advanced testing based on TLPT. The Authority is currently working on the adoption and implementation of the TIBER-EU framework in Malta, within the context of the implementation of the DORA Regulation as outlined in the Consultation on the Adoption of the TIBER-EU Framework in Malta, published by the Authority in March

2023. The Feedback Statement on the Adoption of the TIBER-EU Framework in Malta was also subsequently released by the Authority in February 2024.

In relation to the management of ICT Third Party Risk, Financial Entities will be required to have standard contractual provisions within their contractual arrangements with TPPs. They will also be required to maintain a RoI, with information about all their ICT TPPs. The DORA Regulation places additional and robust requirements for those designated as CTTPs at a Union level. These CTTPs will be subject to direct EU oversight with an element of national follow-up by the relevant competent . More detail on the designation process of the CTTPs is described in sub-section titled *'ICT Third-Party Risk'* of this Nature and Art document.

The last pillar regulates the voluntary participation of Financial Entities in information-sharing arrangements set between themselves with a view to increase resilience by exchanging information on cyber threats and intelligence. More information can be found under Circular titled Information Sharing Arrangements under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, released by the Authority in April 2024.

The DORA Regulation is proportionate by design, and based upon four proportionality layers built upon each other, respectively: (1) exceptions to scope as specified in Article 2(3) of the DORA Regulation; (2) the proportionality principle, in which entities are required to apply the relevant requirements of the Regulation taking into account their size, risk profile, nature, scale and complexity of their services, activities and operations; (3) microenterprises being excluded from an element of requirements and/or benefit from lighter requirements, as applicable; and (4) Article 16 entities being also excluded and/or benefit from lighter requirements, as applicable.

Major ICT-Related Incident Reporting and Management and Significant Cyber Threat Notification and Management

Reporting and Management of Major ICT-Related Incidents

As Financial Entities are increasingly relying on ICT to conduct their business, and as ICT risk continues to pose significant challenges to the resilience, performance, and stability of the financial system, preparedness towards dealing with ICT-related incidents is essential. In October 2022 the SIRC function has, following a comprehensive consultation process, published a circular titled Reporting of Major ICT-Related Incidents, outlining the Authority's expectations in relation to the reporting and managing of Major ICT-Related Incidents by all eligible Authorised Persons. The purpose was to standardise the process by which Authorised Persons classify and report Major ICT-Related Incidents to the Authority. This is also with a view to prepare Authorised Persons for compliance with Chapter III of the DORA Regulation on ICT-Related Incident Management, Classification and Reporting.

The SIRC function has made available the following material to Authorised Persons on the Authority's website within the SIRC webpage:

1) A Major ICT-Related Incident Reporting Process Document ('the Process Document');
2) Templates for Initial, Intermediate and Final Major ICT-Related Incident Reporting ('the Templates', 'the provided Templates');
3) User Guidelines Document for submitting Major ICT-Related Incident Reports to the Authority ('the User Guidelines').

The Authority expects all eligible Authorised Persons to report Major ICT-Related Incidents, whether of an operational or security nature, to the Authority, in line with the process document, using the provided Templates, and by following the User Guidelines.

In conjunction with the publication of the material on reporting and managing Major ICT-Related Incidents, the SIRC function has made a new functionality available to eligible Authorised Persons within the Licence Holder Portal. This new functionality is the new incident reporting management system, which all eligible Authorised Persons are expected to make use of, for the reporting of Major ICT-Related Incidents. The system requires Authorised Persons to fill out and submit the provided templates mentioned previously. Further information on how to make use of the System is provided in the User Guidelines for Submitting Major ICT-Related Incident Reports, as published by the Authority in October 2022.

In preparation for the date of applicability of the DORA Regulation, the Authority is currently working on updating its current incident reporting management system to be aligned with the requirements of the DORA Regulation. The Authority will communicate any developments regarding the update of its current incident reporting management systems via the appropriate channels. For additional information, stakeholders are invited to refer to two episodes within the Authority's DORA Videocast series, namely ICT-Related Incidents under DORA and The Interplay Between Different Incident Reporting Mechanisms and DORA.

Significant Cyber Threat Notification and Management

Authorised Persons and relevant parties may, on a voluntary basis, relay to the Authority notifications of Cyber Threats via the appropriate channels. The Authority has been made aware of several Cyber Threats, most noticeably phishing and smishing attacks, third-party vulnerabilities and denial of service attack attempts.

Once the DORA Regulation becomes applicable (17 January 2025), Financial Entities may notify the Authority of Significant Cyber Threats, in accordance with the requirements of that Regulation. The Authority will communicate any developments regarding the mechanism for the voluntary notification of Significant Cyber Threats via the appropriate channels.

Prevalent Threats in 2023

Following the analysis of the information gathered locally and from other competent authorities, the SIRC Function would like to shed light on prevalent cyber threats in 2023, as follows:

- **Social engineering, more specifically phishing, smishing and clone websites created with a view to mimic legitimate websites of Financial Entities.** The Authority, upon becoming aware of clone websites, contributes towards building awareness via the publication of publicly available warnings.
- **Unauthorized access through multi-factor authentication fatigue techniques**. Multi-factor authentication that contains a 'number matching feature', instead of an 'accept' push notification only, can be one form of control[4].
- **Third-Party vulnerabilities affecting Authorised Persons.** In this context, Authorised Persons should, *inter alia*, continuously monitor the services being provided by ICT TPPs, the ICT TPP's compliance with agreed service levels, compliance with any other contractual and regulatory requirements, and adequately manage their ICT third party risk.
- **System failure, more specifically software/application failure**. Authorised Persons should ensure that their systems, software and applications are adequately resilient to failure, and that changes are properly managed and controlled.
- **Ransomware attacks**, a type of security incident through which a threat actor, for instance, encrypts the victim's data and offers the decryption key in return for a ransom. Adequate cyber hygiene reduces the probability of a successful ransomware attack[5].

The SIRC Function would like to also highlight that Authorised Persons must not limit their awareness to only the above-mentioned threats and must also take into account on-going changes to the threat landscape they operate in. In this context, Authorised Persons' participation in information-sharing arrangements is highly encouraged.

[4] Cybersecurity and Infrastructure Security Agency, 'Implementing Phishing-Resistant Multi Factor Authentication'.
[5] European Central Bank, 'Ransomware: oversight perspective for financial market infrastructures'

More information can be found under section titled '*Information-Sharing Arrangements'* to this document.

Cyber Resilience Exercises ('CREs')

CREs simulate extreme but plausible ICT-related incident scenarios and are designed to evaluate detection, response, and recovery strategies and overall incident preparedness, all of which are essential for ensuring a high level of digital operational resilience. The Authority intends to conduct CREs across three focus levels: internal focus through the performance of internal tabletop exercises within the Authority; micro focus via engagements with Authorised Persons; and macro-focus by aligning with national and EU-level initiatives in the area.

Internal Focus

From an internal perspective, CREs can help to gauge and contribute towards sectoral readiness in the event of systemic ICT-related incidents affecting Authorised Persons. In this case, the exercises will be devised in a manner where the Authority will assess the response and possible impact that a scenario-based ICT-related incident may have on the financial services sector. By doing so, the Authority can proactively contribute towards its own detection, response, recovery and preparedness *vis-à-vis* incidents affecting Authorised Persons.

Micro Focus

On a micro level, the focus is on Authorised Person's response to ICT-related incidents. In this context, CREs are conducted in the form of detailed questionnaires designed to assess Authorised Persons' response, recovery and preparedness to extreme but plausible scenarios. Results from these exercises are captured in a final report, which is then disseminated to the relevant Authorised Persons, thereby enhancing sector-wide resilience.

Macro-Level Focus

At the macro level, the Authority is aligning with national and EU initiatives to enhance systemic cyber resilience. The Authority, in collaboration with other national authorities, is currently implementing the tools featured in the Advancing

Macroprudential Tools for Cyber Resilience report, published by the ESRB in 2023, at a national level. This collective effort aims to assess and enhance the financial services sector's capabilities to withstand systemic cyber events that could threaten financial stability. A key component of this project involves understanding and establishing SITOs, which serve as critical benchmarks for gauging the sector's ability to respond and recover from systemic cyber events.

Coordination Frameworks

The aim of coordination frameworks is to strengthen coordination and the level of preparedness between the MFSA and other relevant competent authorities, including the ESAs, in case of a systemic cyber event. At a European level, the ESRB recommended the establishment of a coordination framework titled EU-SCICF[6]. The aim of this framework is to ensure dialogue between financial authorities with a view to facilitate coordination in case of a major systemic cross border cyber event, and also to mitigate the risks of such event taking place.

More specifically, the objective of the EU-SCICF is to facilitate an effective Union-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the Union's financial sector. The establishment of the EU-SCICF will contribute towards greater levels of coordination, communication, in addition to the early assessment of a major cyber event, effective response and recovery measures and limitation of contagion, from a financial stability perspective.

At a national level, the NCSC is implementing a national coordination framework for operational coordination amongst relevant identified stakeholders in the public service for the purposes of, *inter alia*, handling a cyber security response on a national scale, in accordance with action 2.2 of the National Cybersecurity Strategy 2023-2026.

[6] See ESRB Recommendation of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities.

ICT Risk Questionnaires and Horizontal Analyses

As part of its ongoing supervisory efforts, the SIRC Function engages with supervised entities through ICT Risk Questionnaires. The objective of this Questionnaire is to ensure that Authorised Persons have in place adequate internal governance and control frameworks and, more generally, an appropriate digital operational resilience posture.

In 2023 the Authority engaged with a sample of Authorised Persons taking into account the industry's level of alignment with the Guidance Document and the level of industry preparedness for the DORA Regulation. In 2024 the Questionnaire aligns with and contributes towards the SIRC Function's set supervisory priorities and its efforts towards outcome-based supervision, as already outlined in this document.

The Questionnaire is a cross-sectoral horizontal analysis tool consisting of questions pertaining to key ICT themes, namely: ICT Governance and Strategy; ICT and Security Risk Management; Information Security; ICT Operations Management; ICT Business Continuity; ICT Project and Change Management; ICT Business Continuity; ICT Project and Change Management; ICT Third-Party Service Providers; and DORA Preparedness. A cross-sectoral sample has been chosen to undergo the 2023 Questionnaire (refer to Figure 4).

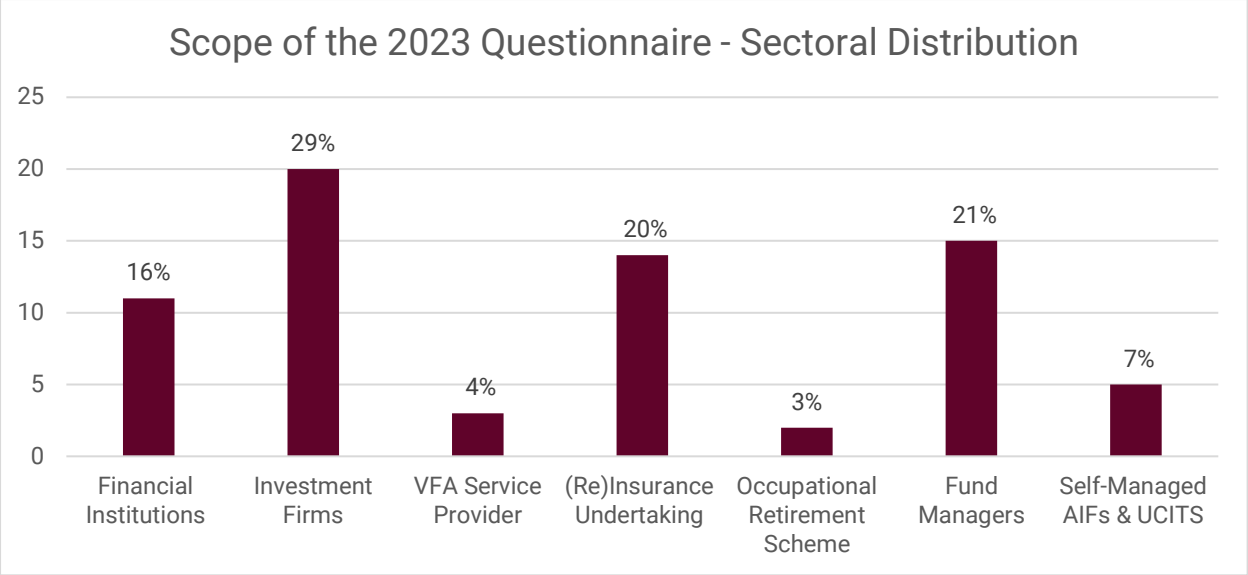

Figure 4: Scope of the Questionnaire

Data quality checks were carried out on all questionnaires submitted to the Authority. Where errors were identified, respondents were asked to re-submit their questionnaire. Ensuing these data quality checks, a risk rating methodology has been applied to the data set where each answer has been given a weighted score. Subsequently, risk-weighted scores were applied to each question, theme and overall risk rating. This has ultimately determined the overall risk rating for each Authorised Person in scope, in addition to a sectoral risk rating for each theme (Figure 5).

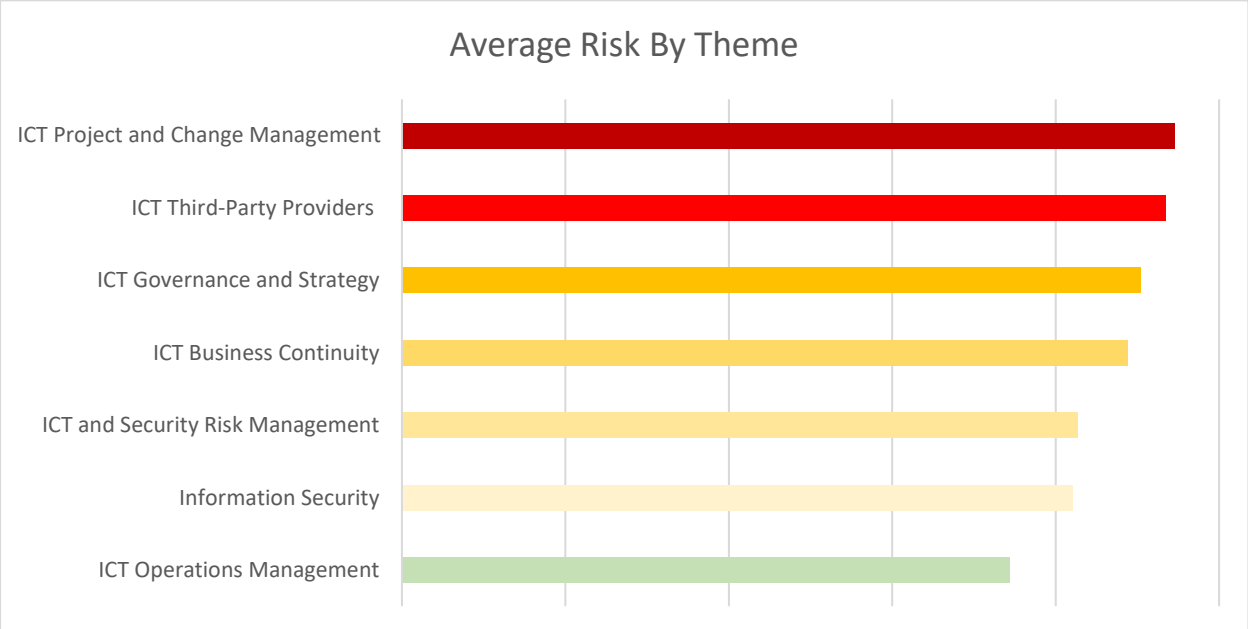

Figure 5: Average Risk by Theme

The results outlined in Figure 5 suggest that, the areas where the industry lacks the most, in terms of adequate measures, controls and overall alignment with current applicable regulatory provisions, relate to: ICT Project and Change Management; and the management of ICT Third Party Risk.

In terms of ICT Project and Change Management, Authorised Persons should take the necessary steps to ensure that they identify, assess and manage risks deriving from the portfolio of ICT projects, including risks that are the result of interdependencies between different projects and from dependencies of multiple projects on the same resources. Authorised Persons should also ensure that they identify, assess and manage the risks arising from the use of ICT TPPs and their supply chain. It is important to note that Authorised Persons remain fully responsible and accountable for complying with all of their regulatory obligations and for ensuring that they continue to meet, on an ongoing basis, all regulatory obligations.

On the other hand, the data suggests that the best scoring was obtained in the area of ICT Operations Management. This would imply that Authorised Persons manage their ICT operations via documented and duly implemented internal processes and procedures, which have been approved by the company's management body. They have also documented and implemented policies with a view to operate, monitor and control their technology arrangements, including documenting their critical ICT operations.

The SIRC Function will continue to engage with Authorised Persons with a view to contribute towards the enhancement of their internal controls, alignment with regulatory requirements and their digital operational resilience.

Supporting Authorisations

As part of its cross-sectoral duties, the SIRC Function supports sectoral supervisory functions during the authorisation process. The SIRC Function provides observations and recommendations on the digital operational resilience posture of an Applicant seeking authorisation or a Financial Entity that is already authorised but seeking further authorisation/s (the 'Applicant'). For more information on the authorisation process, interested stakeholders are invited to refer to the Authority's Authorisation Process Service Charter.

The SIRC Function assesses relevant material submitted by an Applicant against applicable benchmarks emanating from the relevant legislative and regulatory frameworks. *Inter alia*, these assessments are carried out taking into account key themes, such as ICT Strategy, ICT and Security Risk Management, ICT Governance, ICT Technology Arrangements, ICT Third Party Risk and Business Continuity Management. The thoroughness and scope of an assessment depends on the nature of an Authorisation, the stage at which an Authorisation is received, the Applicant's associated sectoral risk and the principle of proportionality.

Throughout 2023, the SIRC Function experienced a significant increase in the number of authorisations processed. The SIRC Function has been particularly involved in authorisations associated with Credit Institutions, Financial Institutions, Investment Services Providers, Virtual Financial Assets Service Providers and (Re)Insurance Undertakings. The nature of authorisations has been predominantly related to the new licenses or the notification of a new arrangement with an ICT TPP.

Overall, the SIRC Function has noted strong efforts being taken by Applicants to be aligned with the relevant regulatory and legislative requirements and a high level of awareness in relation to ICT, more specifically on Information Security and ICT Operations Security. However, the SIRC Function has noted shortcomings related to the following:

- **Lack of documentation of an adequate ICT Strategy by the Applicant** and a corresponding implementation plan that is communicated to the relevant stakeholders;
- **Lack of a clear identification of the dependencies of the Applicant's business functions, supporting processes and information assets,** in addition to a lack of a clear identification of which ICT risks impact the said functions, processes and information assets;
- **An insufficient and erroneous understanding and application of the definition of outsourcing**, thereby resulting in lack of alignment with the management of ICT outsourcing risk with respect to critical or important functions that are outsourced;
- **Lack of adequate written contractual arrangements between the Applicant and ICT TPPs**, including a lack of alignment with key contractual provisions outlined in the relevant regulatory and legislative frameworks; and
- **Lack of adequate Business Continuity and Disaster Recovery Plans**, including a lack of documented Exit Strategies.

The SIRC Function will continue to engage with Applicants, especially with a view to ensure that Applicants have a sufficient level of DORA Preparedness, in line with the SIRC Function's outcome-based supervision approach.

Information-Sharing Arrangements

Chapter VI of the DORA Regulation introduces an obligation on Financial Entities within scope to notify the Authority of their voluntary participation in information-sharing arrangements. Information-sharing arrangements are established for the exchange of cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools. Whilst membership per se in such information-sharing arrangements is voluntary, it is however an encouraged practice. More information can be found under Circular titled Information Sharing Arrangements under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, released by the Authority in April 2024.

In addition to the above, the Authority has taken steps towards raising awareness in relation to existing information-sharing arrangements, more specifically the Cyber Threat Intelligence Communication Programme created by the Maltese Government Computer Security Incident Response Team. More information can be found within Circular titled Malta Information Technology Agency – Cybersecurity Projects, released by the Authority in October 2023.

On-Going Supervision

The SIRC Function conducts supervisory engagements to assess the ICT and cybersecurity posture of Authorised Persons using a variety of engagement tools at the disposal of the Authority's supervisory toolkit on an on-going basis and following a risk-based approach. The Authority's supervisory toolkit is made of several tools with different levels of intrusiveness, which are introduced and discussed below.

On-Site Inspections

The most intrusive tool within the Authority's supervisory toolkit is that of on-site inspections. The objective of an on-site inspection is to establish a personal and interactive session with Authorised Persons. The Authority selects which Authorised Persons it will engage with via on-site inspections using a risk-based approach.

During an on-site inspection, experts and professionals in the field of ICT and cybersecurity conduct interviews and meetings to obtain a full and first-hand understanding of the ICT and cybersecurity environment of Authorised Persons. The SIRC Function proportionally and reasonably assesses the controls that Authorised Persons have in place with a view to ensure the containment of ICT risk to an acceptable level whilst promoting cyber-resiliency and preparedness. These obligations are assessed against applicable sectoral legislation and guidelines. To achieve this, corroboration of facts and evidence of Authorised Person's policies, procedures, and guidelines are sought and evaluated against verbal submissions during interviewing sessions and first-hand presentations of the solutions in service within the Authorised Persons' environments.

In view of the DORA Regulation, the Authority has already started adopting its on-site inspection plans to include the assessment of controls that are mandated by currently applicable laws, rules, and guidelines and also have an equivalent corresponding provision of the DORA Regulation. With a view to contribute towards the Financial Entities' transition to compliance with the DORA Regulation, the Authority's post-onsite

inspection report is including a new section for each identified finding which details the corresponding article from the DORA Regulation that would have been breached. To this extent, Financial Entities shall be required to provide a remedial plan which addresses its current shortcomings using provisions emanating from the DORA Regulation.

Thematic Reviews

Another form of engagement that the SIRC Function utilises to ensure the sector's cybersecurity preparedness and resilience is through the use of thematic reviews. Unlike on-site inspections that entail the physical presence of the Authority's representatives within the Authorised Persons' premises, a thematic review is required to be executed by the Authorised Person upon formal notification from the Authority.

A self-assessment by the Authorised Person will be carried out by the instructed persons or function, usually the Authorised Person's third line of defence. The scope, terms, and conditions of the thematic review are provided by the Authority where the controls under assessment are determined following market analysis, trends, and consultations, including with the ESAs, cybersecurity authorities and the private sector. The themes under analysis are grounded in applicable sectoral legislation and applicable guidelines that Authorised Persons should be adhering to. Thus, thematic reviews not only serve to evaluate a particular aspect of cybersecurity, but it also seeks to evaluate the Authorised Person's ability to continually assess itself against prevalent cybersecurity threats which should be duly identified, recorded, and managed by adhering to these legal obligations.

To this extent, the SIRC Function has redesigned its engagement letter and its list of controls to reflect the changes contemplated in the DORA Regulation. As is the case for on-site Inspections, the controls are required in currently applicable laws, rules, guidelines and the DORA Regulation. Additionally, a remedial plan will be requested to include adherence with the DORA Regulation whilst addressing the fulfilment of a control.

Supporting SREP

The SIRC Function assists with the prudential supervision of Credit Institutions via ECB's SREP. Under the SREP methodology the aim is to, *inter alia*, verify that Credit Institutions have the necessary controls and mitigating measures in place.

In the context of SREP, the assessment of the Credit Institution's ICT risk happens against the Applicable Guidelines on ICT Risk Assessment Under SREP (EBA/GL/2017/05). Under SREP, ICT contributes to a wider assessment of the Credit Institution's operational risk score by taking into account factors such as internal governance and ICT strategy, ICT risk management and the identification and proper control of ICT risks.

In this sense, the SIRC Function is requested to review the completed ECB SREP IT Risk Questionnaire potentially together with any of the Credit Institution's ICT-related documentation, and in accordance with the SREP Guidelines. Comments and recommendations emanating from the assessment are relayed to the prudential supervisor who will use the SIRC Function's assessment on the overall scoring of the entity. The SIRC Function also participates in supervisory meetings either during the SREP or after the sharing of the results with the institutions, as applicable.

Supervisory Meetings

Another form of engagement that is used by the SIRC Function is through supervisory meetings. Here, the Authority holds a physical or virtual meeting with Authorised Persons to discuss pertinent cybersecurity matters that require immediate attention.

Dear CEO Letters

Dear CEO Letters are addressed to specific senior members within the organisational structure of an Authorised Person. Dear CEO Letters are important tools towards raising awareness and, more generally, gathering feedback on a particular topic. The SIRC Function has released Dear CEO Letters within the context of the DORA Regulation with a view to contribute towards the Supervisory Outcome of DORA Preparedness, as specified in the MFSA Supervision Priorities 2024 document.

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 in 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.

In March 2024, the Authority published a Dear CEO Letter titled The Authority's Minimum Expectations in Relation to Financial Entities' Preparedness to Regulation (EU) 2022/2554 on Digital Operational Resilience. This Dear CEO Letter contained updated minimum expectations (the '2024 Minimum Expectations'). 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.

Common Findings

During its ongoing supervisory initiatives, as detailed in this section, the SIRC Function has observed four recurrent ICT and cybersecurity shortcomings across the sector. The Authority highly encourages Authorised Persons to take this information into account and consider evaluating their ICT and cybersecurity posture to ensure their adherence. These four common findings have contributed towards the SIRC Function's 2024 Supervisory Priorities and Outcomes, as specified in section '*Our Supervisory Approach*' of this Nature and Art document.

Firstly, 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 adoption of a transition plan, however, is still largely in progress. As the date of applicability of the DORA Regulation approaches, the Authority expects tangible

progress against the 2023 Minimum Expectations. 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. More details on the Authority's 2024 Minimum Expectations on sufficient DORA Preparedness can be found in Dear CEO Letter titled The Authority's Minimum Expectations in Relation to Financial Entities' Preparedness to Regulation (EU) 2022/2554 on Digital Operational Resilience, published by the Authority in March 2024.

Secondly, Authorised Persons recurrently failed in adequately measuring the effectiveness of the controls that are legally mandated. In particular, Authorised Persons were observed to have failed adherence with their own internal policies and procedures. To this extent, the Authorised Person's Risk and Compliance Function should ensure that it adheres to an approved plan to continuously assess its controls. These plans should be accompanied with the necessary internal approvals, such as those from the Management Body, whilst adherence and fulfilment of the checks mandated in these plans should be easily ascertainable by the Authorised Person's internal and/or external audit or by enquiry from the Authority, as requested.

Thirdly, Authorised Persons should step up their efforts to ensure adherence and alignment to an incident management lifecycle that aims to decrease downtimes as much as possible. Lastly, Financial Entities in general did not gain enough momentum in ensuring that their ICT TPP contractual arrangements are going to be in line with the DORA Regulation before its date of applicability. To this extent, Financial Entities should start renegotiating the terms of their ICT TPP contractual agreements to ensure that they adequately cover digital operational resilience in preparation for DORA. On this note, ICT TPPs are also encouraged to ensure alignment of the contractual agreements that they have in place with Financial Entities that are in scope of the DORA Regulation.

ICT Third-Party ('ICT TPP') Risk

Register of Information

Pursuant to Chapter V of the DORA Regulation, Financial Entities within scope will be required to maintain and keep updated a RoI containing information on all their contractual arrangements entailing the use of ICT services provided by ICT TPPs. The RoI needs to be established and kept in accordance with the Technical Standard specifying the RoI standard templates, referred to in Article 29(9) of the DORA Regulation.

The rationale behind the RoI is two-fold. Firstly, the RoI is an important tool for day-to-day ICT TPP risk management within a Financial Entity. Secondly, the aggregate data emanating from the RoIs will allow the ESAs to designate CTPPs, which will be subject to the Oversight Framework established under Chapter V Section II of the DORA Regulation. Considering the above, Financial Entities will be required to report the full RoI to the Authority once the DORA Regulation becomes applicable (17 January 2025). The SIRC Function is closely working with the ESAs with a view to contribute towards Financial Entities' preparedness *vis-à-vis* the reporting of their RoIs through, *inter alia*, participation in relevant *ad hoc* exercises. Indeed, *ad hoc* exercises involving the collection of RoIs from selected Financial Entities have continuously taken place since 2022, the latest of which has been communicated by the Authority via Circular titled Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector: 'Dry-Run' 2024 *ad hoc* Exercise on the Data Collection of Registers of Information, published in April 2024.

Through the *ad hoc* exercises conducted, it has been noted that the industry should seek to ensure full visibility of the ICT TPPs contracted, including visibility on the supply chain (that is, sub-contractors). Ensuring visibility also contributes towards the Financial Entity's sufficient DORA Preparedness, in line with SIRC's outcome-based supervision approach.

Oversight Framework of Critical Third-Party Service Providers

The ESAs, upon analysing the data submitted via the RoIs, will designate ICT CTPPs in line with the Commission Delegated Regulation supplementing Regulation (EU) 2022/2554 by specifying the criteria for the designation of ICT third-party providers as critical for financial entities [not yet in force]. ICT CTPPs are those ICT TPPs which are considered to be of critical importance to Financial Entities across the Union, in accordance with the designation criteria established by Article 31(2) of the DORA Regulation.

The CTPPs will be subject to an Oversight Framework established by Chapter V Section II of the DORA Regulation. The Lead Overseer is the primary contact point for oversight matters related to CTPPs. According to Article 33(2) of the DORA Regulation, the Lead Overseer assesses whether the CTPP has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk which it may pose to Financial Entities.

Competent authorities, such as the MFSA, have a dual role to play in the Oversight Framework established by the DORA Regulation. Oversight cooperation between the ESAs and competent authorities are guided by the Joint Guidelines on the oversight cooperation and information exchange between the ESAs and the competent authorities under Regulation (EU) 2022/2554 [not yet adopted and not yet in force].

Firstly, competent authorities play a key role in the Oversight Framework by means of contributing and participating in the Joint Examination Teams, which are responsible for conducting investigations and inspections of CTPPs, in accordance with Article 38(1) of the DORA Regulation; and the Oversight Forum for the purposes of, *inter alia*, promoting coordination measures, as established via Article 32 of the DORA Regulation. Competent authorities can also take direct measures concerning CTPPs, but only in agreement with the Lead Overseer. The Authority intends to participate in such investigations and inspections, as relevant.

The second role that competent authorities play in relation to the Oversight Framework is *vis-à-vis* the follow-up of recommendations by the Lead Overseer, as specified in Article 42 of the DORA Regulation. In this context, upon the issuance of a

recommendation by the Lead Overseer to a CTPP, the Authority is responsible for the follow-up concerning the risks identified in that recommendation, where they concern Financial Entities making use of the services provided by the CTPP. In other words, Financial Entities should adequately manage their ICT TPP risk, including where it concerns risks identified by the Lead Overseer in the context of CTPPs. In turn, the Authority should take measures to ensure that appropriate risk management is being applied.

Considering the above, the SIRC Function is currently working on establishing the necessary internal structure and procedures, in line with relevant Guidelines emanating from the DORA Regulation, to be able to fulfil the relevant roles within the context of the Oversight Framework of CTPPs.

Threat-Led Penetration Testing

The DORA Regulation introduces a legislative framework aimed at ensuring the digital operational resilience of the financial sector in the EU. Although the DORA Regulation puts in place requirements for general testing of ICT systems for all Financial Entities within scope, selected Financial Entities will be required to also undergo advanced testing based on TLPT. The DORA Regulation's approach to TLPT is aligned with the goal of ensuring that core subsectors and entities that play a systemic role in the financial system have robust cybersecurity measures in place, capable of protecting against, and responding to, ICT-related disruptions and threats. DORA TLPT is to be supplemented by a regulatory technical standard, developed in accordance with the TIBER-EU Framework.

TIBER-EU is a specific testing framework developed by the ECB to provide a standardised approach to conducting red-teaming tests across EU member states. These tests are designed to mimic the tactics, techniques, and procedures of real-life cyber adversaries, aiming to test the resilience of Financial Entities against sophisticated cyber-attacks. TIBER-EU facilitates a controlled environment where attacks can be simulated on critical live production systems without causing harm, allowing institutions to assess their defences and response mechanisms accurately. The adoption of the TIBER-EU framework is voluntary by Member States.

Under the DORA Regulation, the adoption of DORA TLPT is mandatory for both Member States and those Financial Entities selected to undergo these tests. Because DORA TLPT is a legal requirement, it should prevail over the TIBER-EU framework due to its voluntary nature. However, the requirements of DORA TLPT prescribed by the relevant regulatory technical standard have been drafted in accordance with TIBER-EU. The Consultation Paper on Draft Regulatory Technical Standards specifying elements related to Threat-Led Penetration Testing provides further insight on the approach followed by the ESAs in relation to the differences between TIBER-EU and DORA TLPT. Interested stakeholders are invited to refer to sections 3.2.2 and 3.2.3 of the Consultation Paper mentioned above for further guidance.

Updates from the MFSA

With a view to gather industry feedback from relevant stakeholders, the Authority released a Consultation on the Adoption of the TIBER-EU Framework in Malta, in 2023. A Feedback Statement on the Adoption of the TIBER-EU Framework in Malta, detailed the feedback gathered in the Public Consultation and, where applicable, the Authority's response. In addition, questions pertaining to DORA TLPT have been answered via the Feedback Statement to Queries Raised by Consulted Stakeholders on Regulation (EU) 2022/2554 on Digital Operational Resilience (the 'DORA Regulation'), published by the Authority in 2024. For more practical guidance, stakeholders are invited to refer to two episodes of the Authority's DORA Videocast series, namely Digital Operational Resilience Testing Programme & Advanced Testing and More on DORA's Advanced Testing and TIBER-EU. Interested stakeholders are invited to refer to all of the above-mentioned material released by the Authority.

The MFSA is currently working on the national implementation of DORA TLPT, in line with the relevant regulatory technical standard. The Authority will continue to keep stakeholders updated in relation to any relevant developments. In addition, a revision of the current TIBER-EU framework, aligned with the respective Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554 [not yet adopted and not yet in force] is expected to be released in due course. The Authority also intends to implement the said updated version of the TIBER-EU framework.

Outreach

Building upon Strategic Priority 10 and in preparation to the upcoming date of applicability of the DORA Regulation in January 2025, the SIRC Function has engaged in comprehensive outreach initiatives. The SIRC Function's outreach activities aimed at contributing towards not only Authorised Persons' awareness, but also industry-wide awareness, such as relevant associations, consultants, and tertiary students.

The Function kept Authorised Persons updated on developments related to the DORA Regulation via several Circulars published by the Authority, as cross-referenced throughout this Nature and Art document.

Regarding stakeholder consultation and engagement, the Function carried out an informal consultation with the SMEs Chamber and delivered an information session to senior staff within the Chamber of Commerce. With a view to gather industry-wide feedback, the SIRC Function sent letters to several sectoral associations in Malta, asking them to consult with their members and raise any issues and/or feedback to the Authority they might have in relation to the DORA Regulation. The Authority's reply to the questions asked by stakeholders within the associations has been made available via the Feedback Statement to Queries Raised by Consulted Stakeholders on Regulation (EU) 2022/2554 on Digital Operational Resilience (the 'DORA Regulation'), published in February 2024.

The SIRC Function also explored alternative ways in which it could carry out outreach activities. In this vein, the Function has released a periodic videocast series on the DORA Regulation. Lastly, the Function partnered with stakeholders and delivered several presentations and information sessions to associations and consultants; in addition to presentations at the University of Malta, which targeted tertiary students.

The intensive outreach initiatives generated several questions from stakeholders. The SIRC Function centralized questions it received in 2023 via the creation of a FAQs section on its webpage (available under the legislation sub-page).

Concluding Remarks

The SIRC Function has sought to mature its underlying activities and processes since its establishment in 2020. In this context, the establishment of the DORA Regulation has served (and continues to serve) as an important foundational pillar for these activities and processes.

The core supervisory processes (such as authorisations and on-going supervision) have been streamlined and follow a risk-based approach. In addition, the SIRC Function has also committed itself to an outcome-based supervisory approach and has been using several tools within its supervisory toolkit to contribute and ensure Authorised Persons' progress against key supervisory priorities, namely sufficient DORA Preparedness, implementation of strong risk management and compliance functions, adequate incident management processes and satisfactory status of ICT TPPs. Away from micro-prudential supervision, the SIRC Function has also taken steps towards engaging in cyber-risk management, as an integral part of macro-prudential supervision and financial stability – as seen in processes such as Coordination Frameworks and Cyber Resilience Exercises.

From a policy and legislation management perspective, the SIRC Function has been working on the national implementation of the DORA Regulation and national transposition of the DORA Amending Directive. This has been supported by strong outreach efforts, via active engagement with Authorised Persons, national and even international fora.

In the coming years, the SIRC Function will continue to achieve greater streamlining of its processes and continue to contribute towards the digital operational resilience of the Maltese financial services sector, within the framework of the DORA Regulation.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt