MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

9 June 2026

General Observations on Digital Operational Resilience in Authorisation Applications Received in 2025

This Circular applies to Financial Entities and to current and future Applicants whose licence falls and/or will fall within the scope of the DORA Regulation.

In 2025, the Supervisory ICT Risk and Cybersecurity (the "SIRC") Function within the Malta Financial Services Authority (the "Authority") reviewed and processed a number of requests for authorisation, primarily tasked with overseeing the Authority's Annex 05 ("AX05") and Annex 50 ("AX50"). We extend our sincere appreciation to those Applicants who submitted their applications and notifications in a timely and comprehensive manner.

Through this Circular and to guide future potential Applicants, SIRC will be outlining key observations that were noted during the processing of requests for authorisation in 2025.

We would like to draw attention to the expectations when Applicants are compiling and submitting AX50. Where an ICT third-party provider is intending to provide ICT services which will support any critical or important functions of the Applicant or Licence Holders as defined under DORA, Applicants and Licence Holders alike are reminded to carefully assess the applicability of the relevant requirements prior to submitting an AX50. In particular, Applicants should take into account the guidance provided in the **EIOPA FAQ**, which outlines circumstances under which an exemption may apply where the ICT third-party provider also qualifies as a regulated financial entity. Where the conditions set out in the **EIOPA FAQ** are fulfilled, the submission of AX50 may not be required.

We also take this opportunity to inform the public that following internal consultation and recommendations from the sector, as of December 2025, SIRC has published updated versions of the annexes that should be used by Applicants. The newly streamlined format that has been adopted acts as a self-assessment that Applicants must carry out during their compilation. Hence, to facilitate a smooth transaction between Applicants and the Authority, and to reduce the burden on the resources required by both parties without compromising the information required by the Authority to process an application, the Authority's expectations as to the documentation and information that should accompany these annexes have been provided *a priori* by means of Addendums to the Annexes.

The updated annexes can be found here and here.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

A note on generative artificial intelligence ("Gen AI"): The following is consistent with the broader trend identified during the 2025 authorisation cycle, where several submissions lacked sufficient tailoring to the Applicant's operational reality. SIRC recognises that Applicants may use Gen AI to support the preparation of documentation submitted during the authorisation process. When applied responsibly, such tools can assist with drafting and structuring content. However, recent submissions indicate an excessive reliance on AI-generated material that has not been reviewed, validated, or adapted accordingly. This has resulted in documentation that is generic, inaccurate, or misaligned with the Applicant's actual operations and risk profile.

Applicants are reminded that the authorisation process requires clear evidence of understanding, ownership, and tailoring of all submitted policies, procedures, and annexes. Sole dependence on AI tools does not reflect the level of diligence, risk awareness, or attention to detail expected from entities seeking authorisation. While Gen AI may support internal drafting, the ultimate responsibility for the accuracy, completeness, and applicability of all submissions rests with the Applicant, and insufficiently validated content may lead to delays due to resubmissions.

Executive Summary

The 2025 authorisation cycle revealed that while Applicants are increasingly attentive to digital operational resilience, several areas continue to present material challenges. Applicants continue to face the greatest challenges under DORA Chapter II, where many submissions lack the foundational elements of a comprehensive ICT risk management framework. As noted in the Circular, several Applicants failed to provide sufficiently comprehensive ICT business continuity policies and plans, response and recovery plans, and business impact analysis, and often omitted essential components such as a documented digital operational resilience strategy or adequate backup and restoration methods. These shortcomings are mirrored in the Regulatory Technical Standards on the ICT Risk Management Framework, where persistent gaps in ICT business continuity management, asset management, and vulnerability and patch management demonstrate that operational discipline and practical implementation remain insufficiently embedded. Under DORA Chapter II, preparedness is generally stronger, yet weaknesses persist in establishing integrated processes for detecting, managing, and recording ICT-related incidents, with recurring deficiencies in incident classification and reporting.

In contrast, DORA Chapter IV shows the highest level of compliance, with very few observations and no material concerns, which reflects strong alignment with digital operational resilience testing requirements. However, DORA Chapter V remains the second most challenging area, as Applicants continue to underestimate the risks associated with ICT third-party arrangements. Difficulties persist in applying the general principles of third-party risk management and in negotiating the mandatory Key Contractual Provisions. These

issues are reinforced by the Regulatory Technical Standards on the ICT Third-Party Policy, where Applicants frequently fail to conduct proportionate due diligence or to develop tailored exit plans for individual providers.

Overall, the observations across the DORA main text chapters and the Level 2 texts indicate that while progress is evident, many Applicants have not yet achieved the level of maturity required to demonstrate fully embedded digital operational resilience. The Authority emphasises that these shortcomings stem not only from documentation gaps but also from an insufficiently mature understanding of the practical application of DORA requirements. This highlights the need for earlier alignment and more tailored implementation efforts by those Applicants preparing submission for 2026.

Authorisations General Observations

The observations outlined in this Circular apply equally to entities seeking authorisation for the first time and to those who are already licenced and are applying for an additional licence or extension of their existing authorisation. Several of the deficiencies identified during the 2025 cycle were observed across both categories of Applicants.

In processing a request for authorisation, which includes the review of application forms and supporting documentation submitted by Applicants, several recurring areas for improvement were observed. While in certain cases, these observations are subsequently addressed and remediated by Applicants, the trends identified at the initial pre-authorisation stage are retained for supervisory and analytical purposes. For ease of reference, these trends have been grouped according to the relevant chapters of the Digital Operational Resilience Act.[1]

DORA Chapter II – ICT Risk Management

At authorisation stage, ICT risk management emerges as the area presenting the greatest challenges for Applicants, although this outcome may also be attributable to the breadth and complexity of DORA Chapter II. In particular, Applicants experience difficulties in relation to response and recovery,[2] the establishment of a comprehensive ICT risk

[1] REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[2] DORA, art. 11.

management framework,[3] identification,[4] protection and prevention,[5] and governance organisation.[6]

In practice, a number of Applicants generally fail to implement sufficiently comprehensive ICT business continuity policies and plans, response and recovery plans, and business impact analyses, with certain key elements often found to be missing or insufficiently documented.[7] Additionally, deficiencies are also observed in relation to the ICT risk management framework, particularly where Applicants do not include, or do not adequately document, a digital operational resilience strategy,[8] together with the supporting strategies, policies, procedures, and relevant ICT protocols and tools.[9] Further concerns are also identified in relation to backup policies and procedures, and restoration and recovery methods.[10]

Overall, quite a handful of Applicants continue to present difficulties in properly drafting and implementing the policies and procedures required under this Chapter. While room for improvement at pre-authorisation stage is expected, SIRC highlights the general expectation that Applicants should attain a minimum level of satisfactory compliance[11] prior to submitting an application for authorisation. This is considered essential especially for those newly established Applicants as it ensures that they are adequately equipped and operationally robust during their initial years of operation with respect to ICT risk and digital operational resilience.

DORA Chapter III – ICT-Related Incident Management, Classification and Reporting

At authorisation stage, SIRC observes that a significant number of Applicants encounter challenges in establishing an effective ICT-related incident management process.[12] These Applicants often fail to put in place appropriate measures, procedures, and processes to ensure consistent and integrated monitoring, handling and recording of all ICT-related incidents and significant cyber threats.[13] In particular, non-compliance is frequently

[3] DORA, art. 6.

[4] DORA, art. 8.

[5] DORA, art. 9.

[6] DORA, art. 5.

[7] DORA, art. 11(1), 11(2), 11(3) and 11(4).

[8] DORA, art. 6(8).

[9] DORA, art. 6(2).

[10] DORA, art. 12.

[11] Kindly refer to the Minimum Requirements Guidelines (Addendum II) of Annex 05.

[12] DORA, art. 17.

[13] DORA, art. 17(2).

identified in relation to the minimum requirements[14] that must be included within the ICT-related incident management process itself.[15] Consequently, deficiencies are also observed in related areas, including the classification of ICT-related incidents and cyber threats,[16] as well as the reporting of major ICT-related incidents and the voluntary notification of significant cyber threats,[17] all of which require further attention.

Overall, while the majority of Applicants demonstrate a satisfactory level of preparedness with respect to ICT-related incident management, classification, and reporting, a number of Applicants fail to adequately define, establish, and implement the necessary processes to detect, classify, manage, and notify ICT-related incidents and cyber threats in line with the requirements of DORA.

DORA Chapter IV – Digital Operational Resilience Testing

At authorisation stage, DORA Chapter IV is the chapter with the highest level of compliance observed. Very few observations are recorded in this area, and no specific points of concern are identified. SIRC notes that the limited observations raised primarily relate to the general requirements for the performance of digital operational resilience testing.[18]

In light of the above, there are no noteworthy observations which need to be highlighted, and SIRC commends the efforts made by Applicants to achieve satisfactory alignment with the requirements of this Chapter.

DORA Chapter V – Managing of ICT Third-Party Risk

As the second Chapter with the highest number of observations, the management of ICT third-party risk remains a recurring area of concern for Applicants. In particular, Applicants experience difficulties in implementing the general principles governing ICT third-party risk management,[19] as well as the 'Key Contractual Provisions' required under DORA.[20]

Applicants seeking authorisation do not always fully appreciate the risks associated with ICT third parties, particularly where such third parties provide ICT services supporting

[14] Kindly refer to the Minimum Supporting Documentation Requirements Guidelines (Addendum III) of Annex 05.

[15] DORA, art. 17(3).

[16] DORA, art. 18.

[17] DORA, art. 19.

[18] DORA, art. 24.

[19] DORA, art. 28.

[20] DORA, art. 30.

critical or important functions. The general principles set out in DORA are designed to ensure that prospective Licence Holders appropriately identify, assess, and manage risks arising from ICT third-party service providers, including prior to the formal conclusion of contractual arrangements.[21]

Furthermore, the 'Key Contractual Provisions' establish a baseline level of safeguards intended to ensure a minimum standard of care in the management of third-party risk. A recurring issue is that Applicants encounter difficulties in negotiating contractual arrangements with prospective ICT third parties to incorporate these provisions, irrespective of whether the ICT services provided support critical or important functions.[22] Applicants should be aware of the ICT, contractual, and operational risks arising from the failure to adequately implement these 'Key Contractual Provisions', in addition to the resulting non-compliance with regulatory requirements.

Overall, this area warrants continued and heightened attention from Applicants and from the industry as a whole. It must be highlighted that, as with all regulatory requirements emanating from DORA, these key contractual provisions are essential for practical reasons rather than solely for regulatory compliance. It is emphasised that the 'Key Contractual Provisions' must be implemented to ensure that arrangements for the provision of ICT services by ICT third-party service providers do not exert an unnecessary risk of adverse effects on the Licence Holder's digital operational resilience. They must be put in place with the intent and understanding that they are there to effectively protect the Licence Holder as party to the contractual arrangement.

DORA Regulatory Technical Standards - Risk Management Framework

With regard to the Regulatory Technical Standards on the ICT Risk Management Framework[23] ("RTS ICTRMF"), it is observed that Applicants experience difficulties in complying with requirements relating primarily to ICT business continuity management,[24] ICT operations security,[25] and ICT asset management.[26]

[21] DORA, art. 28(4), 28(5), 28(7), and 28(8).

[22] DORA, art. 30(2) and 30(3).

[23] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework.

[24] RTS ICTRMF, Chapter IV ICT business continuity management, arts. 24, 25, and 26.

[25] RTS ICTRMF, Chapter I Section 5 ICT operations security, arts. 8, 9, 10, 11, and 12.

[26] RTS ICTRMF, Chapter I Section 3 ICT asset management, arts. 4 and 5.

In particular, Applicants encounter challenges in developing ICT response and recovery plans that adequately take into account the outcomes of the business impact analysis.[27] Difficulties are also observed in the identification and inclusion of all relevant scenarios of severe business disruption when preparing such ICT response and recovery plans.[28]

The development, documentation, and implementation of ICT asset management policies and procedures also emerge as a recurring area of concern.[29] It is frequently observed that these policies and procedures do not prescribe the necessary record-keeping requirements,[30] nor do they sufficiently define the criteria for performing criticality assessments of ICT assets.[31]

Furthermore, vulnerability and patch management constitutes an additional area where Applicants struggle to achieve compliance.[32] Applicants often fail to develop, document, and implement vulnerability management procedures that ensure the effective tracking and verification of vulnerabilities in order to establish and maintain situational awareness.[33] Similarly, patch management procedures are frequently insufficiently documented, particularly with respect to the identification of emergency patching processes and the testing and deployment of software and hardware patches and updates affective ICT assets.[34]

Overall, these observations are consistent with those identified under the main text of DORA. Several of the deficiencies noted in relation to the RTS ICTRMF are intrinsically linked to the broader shortcomings observed in the implementation of DORA requirements. Increased awareness and continued efforts towards satisfactory compliance of this area is required by Applicants.

DORA Regulatory Technical Standards – ICT Third-Party Policy

With regard to the Regulatory Technical Standards on the ICT Third-Party Policy[35] ("RTS ICTTPP"), it is observed that Applicants experience difficulties in complying with

[27] RTS ICTRMF, art. 26(1).

[28] RTS ICTRMF, art. 26(2).

[29] RTS ICTRMF, arts. 4 and 5.

[30] RTS ICTRMF, art. 4(2)(b).

[31] RTS ICTRMF, art. 5(2).

[32] RTS ICTRMF, art. 10.

[33] RTS ICTRMF, art. 10(2).

[34] RTS ICTRMF, art. 10(4).

[35] Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers

requirements relating to the due diligence process[36] and to the exit from and termination of contractual arrangements.[37]

In particular, Applicants encounter challenges in adequately taking into account all the relevant factors when assessing prospective ICT third-party providers. This shortcoming stems both from the absence of sufficiently detailed provisions within the ICT Third-Party Policy itself and from deficiencies in practice, where Applicants fail to evidence that the appropriate and proportionate due diligence has been undertaken prior to onboarding.[38]

When documenting the ICT Third-Party Policy, Applicants also experience difficulties in incorporating a requirement to establish an exit plan for each individual contractual arrangement.[39] Instead, some Applicants adopt a single, generic exit plan intended to apply to all ICT third-party providers. As a result, Applicants frequently fail to consider circumstances that may vary from one provider to another, including: a) unforeseen and persistent service interruptions, b) inappropriate or failed service delivery, and c) the unexpected termination of the contractual arrangement.[40] Such omissions increase the operational and contractual risks associated with the outsourcing arrangement.

These observations further highlight the risks arising from the improper management of ICT third-party risk. In the absence of a comprehensive ICT Third-Party Policy that mandates proportionate due diligence prior to onboarding and requires the establishment of a tailored exit plan for each contractual arrangement, Applicants expose themselves to heightened ICT, operational, and contractual risks, in addition to the risk of regulatory non-compliance.

Conclusion

Overall, the Authority notes that at authorisation stage, Applicants demonstrate varying degrees of preparedness across DORA Chapters and the related Regulatory Technical Standards. While encouraging levels of compliance are observed particularly in relation to digital operational resilience testing and in certain aspects of ICT-related incident management, some significant challenges persist in other core areas. For instance, ICT risk management and the management of ICT third-party risk, together with the requirements emanating from the RTS ICTRMF and RTS ICTTPP, continue to give rise to a substantial number of observations.

The recurring deficiencies identified in this Circular indicate that several Applicants have yet to fully embed digital operational resilience within their organisational frameworks. In

[36] RTS ICTTPP, art. 6.

[37] RTS ICTTPP, art. 10.

[38] RTS ICTTPP, art. 6(1).

[39] RTS ICTTPP, art. 10 para. 1.

[40] RTS ICTTPP, art. 10 para. 1(a, b, c).

many instances, shortcomings stem from documentation gaps as well as from an insufficiently mature understanding of the practical application of DORA requirements, while also keeping in mind the interdependencies between risk management, operational process and contractual safeguards.

The Authority remains committed to engaging constructively with Applicants throughout the authorisation process. Continued industry-wide efforts, further awareness, and proactive alignment with both the Level 1 requirements and the RTSs is crucial in strengthening digital operational resilience and safeguarding the stability and integrity of the financial sector.

The Authority also expects Applicants preparing submissions in 2026 to make full use of the updated annexes and accompanying addenda. Early alignment with these expectations will support a more efficient authorisation process and reduce the need for resubmissions.