

23 October 2026

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

The Board of Directors

Re: Supervisory Engagements and Digital Operational Resilience 2025 - General Observations Report

In 2025, the Supervisory ICT Risk and Cybersecurity (the “SIRC”) Function within the Malta Financial Services Authority (the “Authority”) organised its annual Supervisory Engagement Plan using a variety of Supervisory Engagements Tools with its Licence Holders in relation to Digital Operational Resilience. The Supervisory Engagement Plan was carried out using the Supervisory Engagement Tools detailed in the Authority’s [Supervision Priorities 2025](#). We extend our sincere appreciation for those Licence Holders who were in scope of SIRC’s 2025 Supervisory Engagement Plans and committed the necessary resources to fulfil the Authority’s requirements and expectations.

To complement the supervisory general observations outlined in this letter, Licence Holders are also encouraged to take note of the Authority’s recently issued “[Cyber Threats Awareness Brief](#)”. This brief provides an overview of key cyber threat trends observed throughout 2025 and the first months of 2026, while also providing forward-looking insights relevant to the financial sector. While the circular does not introduce new regulatory obligations, it offers timely situational awareness that should be considered by each Licence Holder for their own ICT risk environment and in the context of Article 8(2) of DORA.

1.0 Executive Summary

This General Observations Report summarises the findings of the SIRC engagements conducted throughout 2025. The assessment covered three core areas aligned with the ESA’s “DORA Day 1” expectations: ICT Risk Management, ICT-related Incident Management, and ICT Third-Party Risk Management. Across all assessed controls, 74% were fully achieved, 16% partially achieved, and 10% not achieved, demonstrating a continued positive trajectory compared to 2024.

The majority of Licence Holders have made meaningful progress in strengthening digital operational resilience, especially in terms of ICT risk identification, incident reporting processes, and the assessment of ICT concentration risk. However, a number of Licence Holders who did not fully achieve the assessed controls have had lingering deficiencies, and this was reflected by those controls which have been scored as partially achieved or not achieved. These gaps include weaknesses in ICT governance and organisation, incident and cyber threat classification, digital operational resilience testing coverage, contractual alignment with DORA requirements, and the practical implementation of the Regulatory

Technical Standards on the ICT Risk Management Framework and the Regulatory Technical Standards on the ICT third-party service providers.

Overall, the sector is moving in the right direction, with clear improvements across DORA Chapters II to V. Nonetheless, further effort is required to ensure consistent implementation, particularly in areas such as change management, encryption and cryptographic controls, access management, and third-party oversight. The Authority remains committed to supporting Licence Holders in achieving full compliance and strengthening operational resilience across the Maltese financial sector.

2.0 Supervisory General Observations

SIRC is pleased to present its general observations following the completion and analysis of data gathered through its 2025 Supervisory Engagement Plan. The Authority is encouraged by the overall findings, which indicate a strong and growing commitment across the Maltese Financial Services Sector towards enhancing digital operational resilience, albeit areas of improvement are being put forward in this letter.

In 2025, SIRC focused on three main areas of supervision which stem from the ESA's "DORA day 1" document.¹

1. The ICT Risk Management Framework, including the required documentation that DORA mandates Financial Entities to have.
2. The Incident Management lifecycle.
3. ICT Third-Party Risk Management.

For all three outcomes in scope of SIRC 2025's Supervisory Engagements, 74% of all assessed controls were rated as fully achieved, 16% as partially achieved, and 10% as not achieved. These results indicate that nearly 90% of all controls were either fully or partially achieved, consistent with the findings of the 2024's assessment. Overall, there has been a clear shift towards full compliance, with a greater proportion of controls now being fully achieved rather than partially achieved. This represents a welcomed improvement and demonstrates that the sector is making meaningful progress in aligning with regulatory expectations.

Despite this encouraging performance by those Licence Holders that have fully satisfied the assessed controls, the Authority has identified recurring areas for improvement that merit sector-wide attention, applicable solely to the subset of Licence Holders falling within the partially achieved and not achieved categories. For ease of reference, these trends have been grouped according to the relevant chapters of the Digital Operational Resilience Act.²

¹ Malta Financial Services Authority, *Supervision Priorities 2025*, pg. 20. <[link](#)>

² 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.

3.0 DORA Chapter II – ICT Risk Management

The Authority observes a positive shift in the way Licence Holders identify and mitigate ICT risks. Figure 2 shows that several key weaknesses highlighted in the Authority’s 2024 Supervisory Engagements were addressed in 2025. Notwithstanding this progress, the latest observations indicate that some of the Licence Holders did not fully achieve the assessed controls pertaining to this Chapter and continue to fall short of the requirements set out in DORA. The most frequently observed gaps are related to identification,³ communication,⁴ response and recovery,⁵ and detection,⁶ as shown in Figure 1 below.

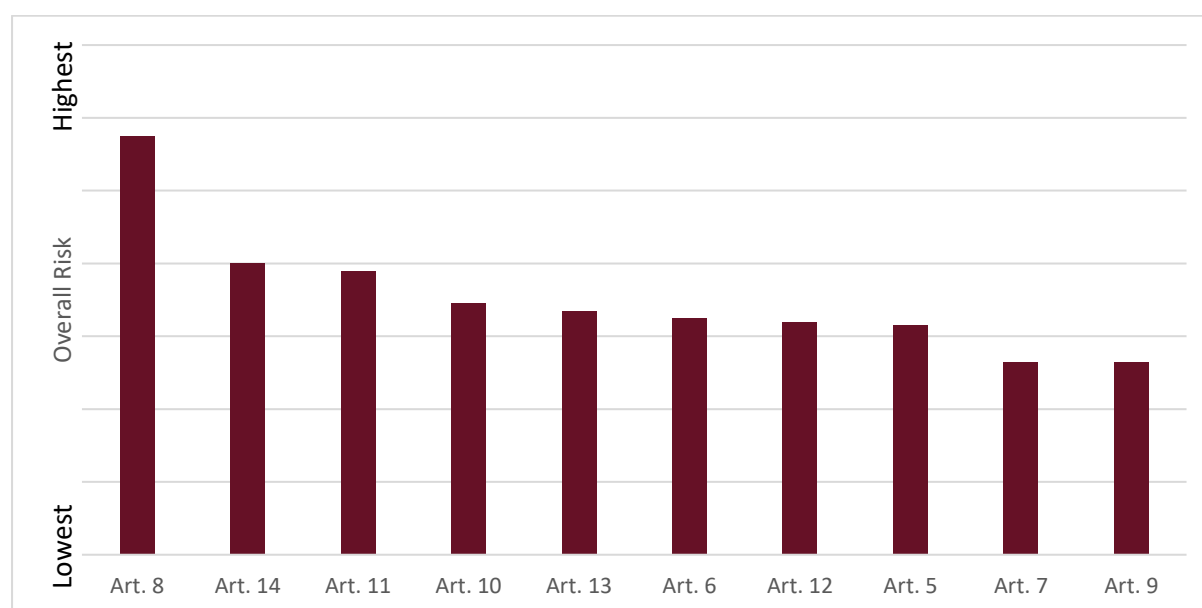


Figure 1 - Bar Chart of the Overall Risk per assessed article of Chapter II of DORA for 2025

At a detailed level, a number of those Licence Holders whose controls for this Chapter were not all fully achieved have experienced particular difficulty in maintaining an appropriate risk register by continuously identifying all sources of ICT risk and assessing cyber threats and ICT vulnerabilities.⁷ Challenges are also noted in the establishing of crisis communication plans responsible for disclosure of major ICT-related incidents, and the implementation of communication policies for internal staff and external stakeholders.⁸ In addition, the Authority observes a lack of regular testing of those mechanisms put in place for the prompt detection of anomalous activities, including ICT network performance issues and ICT-related incidents.⁹

³ DORA, art. 8.

⁴ DORA, art. 14.

⁵ DORA, art. 11.

⁶ DORA, art. 10.

⁷ DORA, art. 8(2).

⁸ DORA, arts. 14(1) and 14(2).

⁹ DORA, art. 10(1) para. 2.

Figure 2 compares the overall risks for 2024 and 2025 and illustrates a general movement towards full compliance, despite isolated increases in overall risk due to non-compliance for some articles.

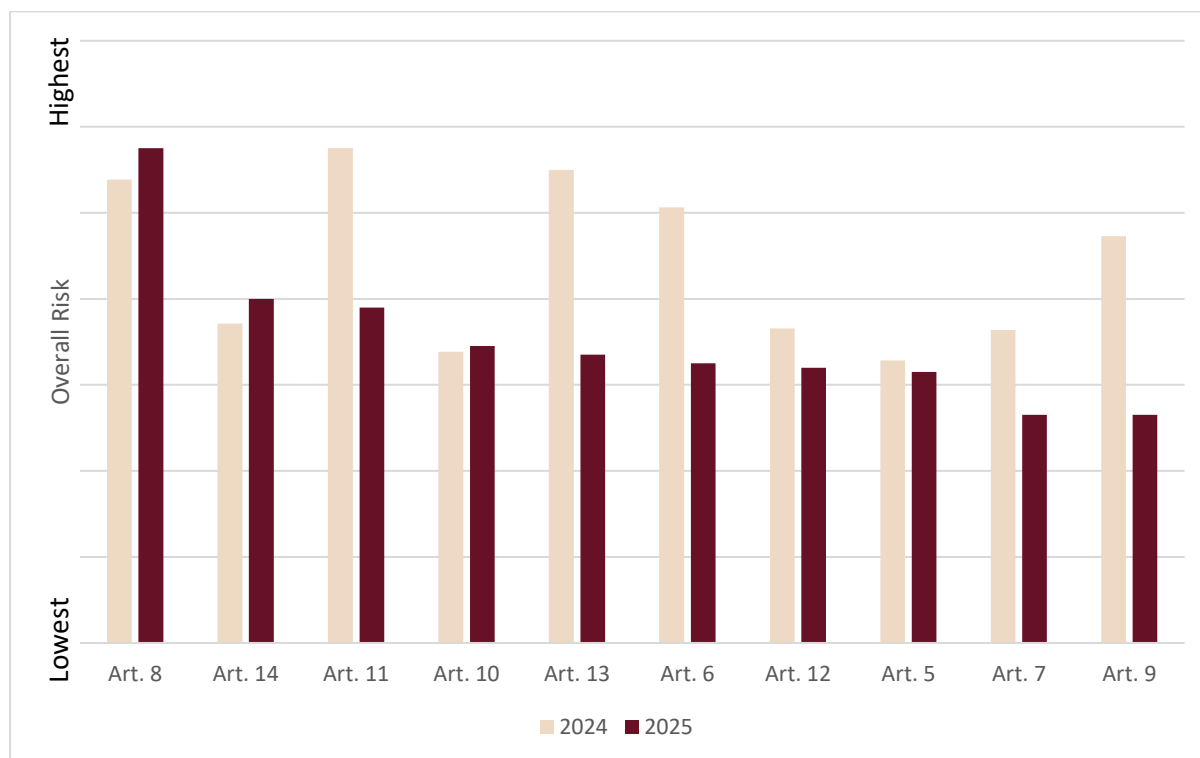


Figure 2 - Bar Chart comparing 2024 to 2025 Overall Risk per assessed article of Chapter II of DORA

While the progress made in 2025 is encouraging, our data clearly indicates that sustained attention to the obligations arising out of this Chapter is essential. Addressing the remaining deficiencies while maintaining the progress already achieved will be critical for ensuring ongoing compliance and strengthening digital operational resilience across the sector from this aspect of DORA.

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

The Authority observes mixed results in relation to ICT-related incident response capabilities. With respect to the ICT-related incident management process¹⁰ and the reporting of major ICT-related incidents and voluntary notification of significant cyber threats,¹¹ Licence Holders registered measurable progress towards meeting regulatory expectations under DORA, as represented by Figure 3 below. Notwithstanding these improvements, a number of those

¹⁰ DORA, art. 17.

¹¹ DORA, art. 19.

Licence Holders that did not fully achieve all the controls for this Chapter continue to experience difficulties in the classification of ICT-related incidents and cyber threats.¹²

In particular, ICT incidents are often not classified in line with DORA requirements, or their impact is not assessed using the prescribed criteria.¹³ In parallel, cyber threats are not consistently assessed and classified as significant based on the criticality of the services potentially affected.¹⁴

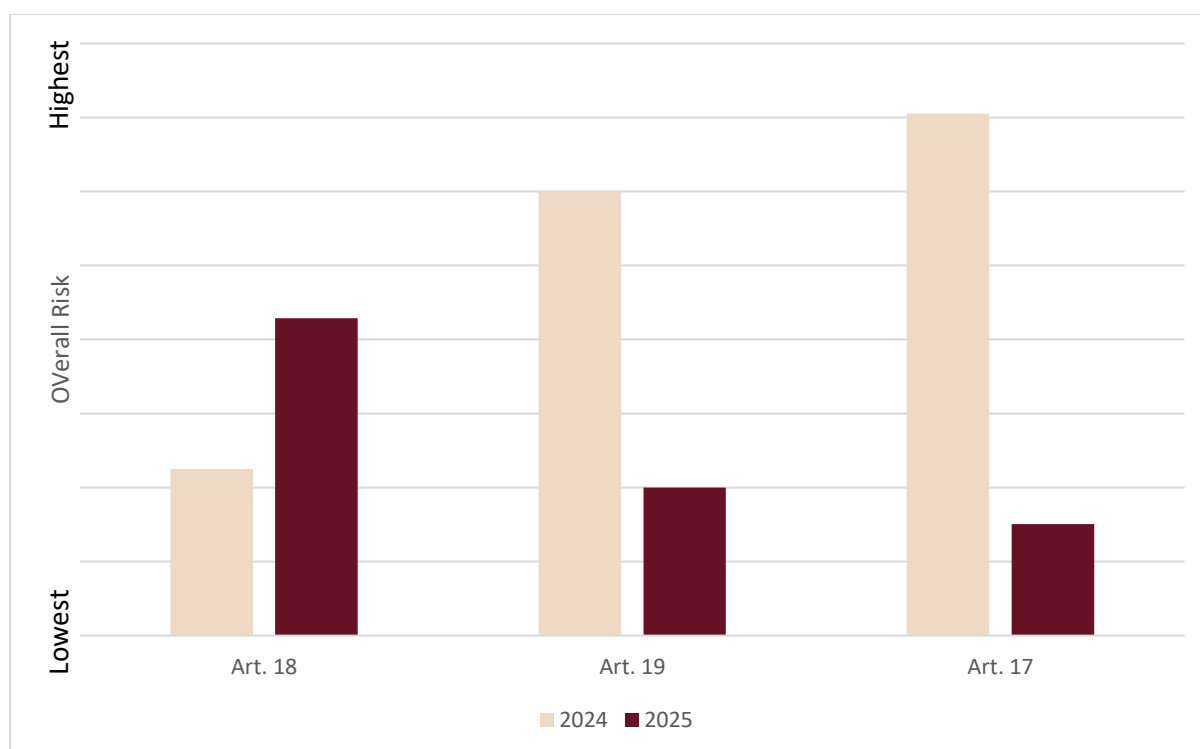


Figure 3 - Bar Chart comparing 2024 to 2025 Overall Risk per assessed article of Chapter III of DORA

These shortcomings weaken the overall effectiveness of incident management frameworks. Inaccurate or incomplete classification may adversely affect the timeliness and quality of incident handling and reporting, increasing the risk that cyber threats are underestimated, insufficiently managed, or not escalated at an early stage to limit potential impact.

5.0 DORA Chapter IV – Digital Operational Resilience Testing

In line with the expectations set out in the Authority's 2024 assessment, a general progression towards more appropriate Digital Operational Resilience Testing practices has been observed across the industry. Licence Holders have demonstrated improvement in meeting the general

¹² DORA, art. 18.

¹³ DORA, art. 18(1).

¹⁴ DORA, art. 18(2).

requirements for the performance of digital operational resilience testing¹⁵ and the testing of ICT tools and systems.¹⁶ Notwithstanding this positive trend, a number of gaps and areas lacking sufficient depth remain evident for a number of those Licence Holders that have not fully achieved the assessed controls.

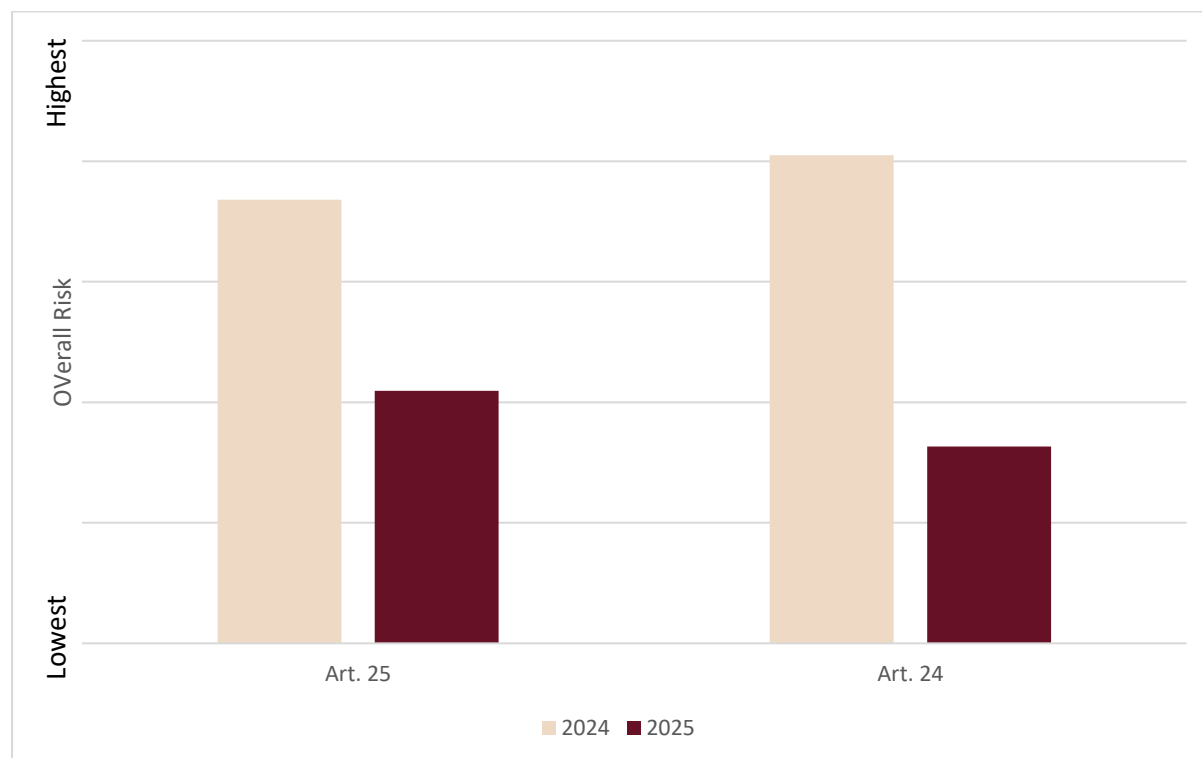


Figure 4 - Bar Chart comparing 2024 to 2025 Overall Risk per assessed article of Chapter IV of DORA

In particular, not all of those Licence Holders have established an approved Digital Operational Resilience Testing Programme as required by DORA.¹⁷ Furthermore, some of those Licence Holders are failing to ensure that appropriate tests are carried out at least annually across all ICT systems and applications supporting Critical or Important Functions.¹⁸

These shortcomings, while limited in scope, remain significant. They indicate that certain vulnerabilities or failure scenarios may not be fully identified or addressed, particularly under stress conditions. Overall, the findings suggest that while testing frameworks are maturing, further effort is required to ensure consistent and comprehensive implementation across all Licence Holders.

¹⁵ DORA, art. 24.

¹⁶ DORA, art. 25.

¹⁷ DORA, art. 24(1).

¹⁸ DORA, art. 24(6).

6.0 DORA Chapter V – Managing of ICT Third-party Risk

The Authority observes that Licence Holders are increasing their efforts towards compliance with the requirements of DORA Chapter V. In particular, as represented by Figure 5, progress has been noted in relation to the preliminary assessment of ICT concentration risk at entity level.¹⁹ This represents an important step towards strengthening oversight of dependencies on external ICT service providers.

Despite these advances, other areas require attention to be given by some of those Licence Holders that have not fully achieved the assessed controls for this Chapter. Most notably, a number of those Licence Holders do not sufficiently align their contractual arrangements with the requirements set out under DORA. This is often due to the incomplete implementation of the Key Contractual Provisions²⁰ and in some cases, the absence of a formal contractual arrangement altogether.²¹

Such deficiencies weaken governance, oversight, and control over ICT third-party providers, including those providing ICT services supporting critical or important functions. In addition, the Authority observes shortcomings in the application of DORA's general principles for the sound management of ICT Third-Party risk.²² These weaknesses may lead to unaddressed dependencies,²³ insufficient audit and access rights, and the reduced ability to ensure continuity, security, and regulatory compliance in the event of ICT-related disruptions.

¹⁹ DORA, art. 29.

²⁰ DORA, art. 30.

²¹ DORA, art. 28.

²² DORA, art. 28.

²³ DORA, art. 28(1)(b)(i).

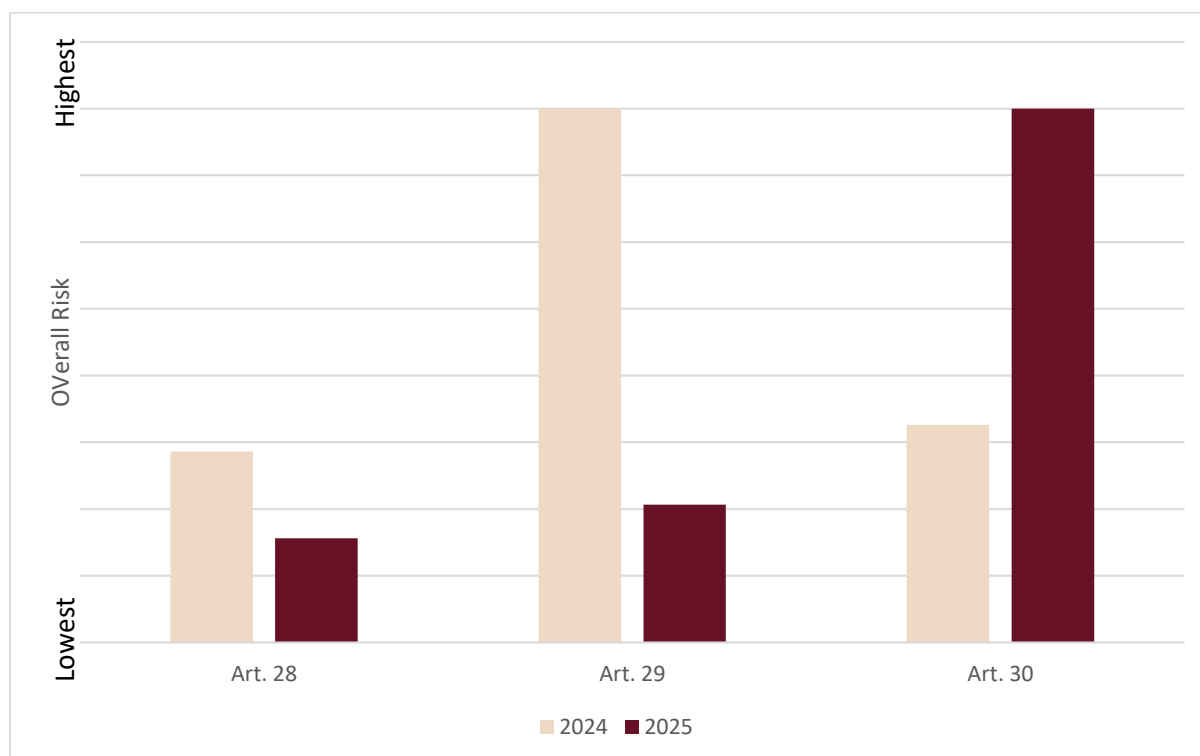


Figure 5 - Bar Chart comparing 2024 to 2025 Overall Risk per assessed article of Chapter V of DORA

Overall, our data indicates that while initial progress is being made, stronger contractual discipline and more consistent third-party risk management practices remain necessary to meet the expectations of Chapter V.

7.0 DORA Regulatory Technical Standards - Risk Management Framework

The Authority observes that Licence Holders are, in general, establishing the foundations of an ICT risk management framework in line with the Regulatory Technical Standards on the ICT Risk Management Framework (the “RTS ICTRMF”).²⁴ However, the practical implementation of this framework remains uneven and, in some cases, not yet sufficiently embedded in the day-to-day operations of some of those Licence Holders who did not fully achieve the controls related to the RTS ICTRMF.

As evidenced by Figure 6, across nearly all areas covered by the RTS ICTRMF, weaknesses are identified to varying degrees. The most notable shortcomings are related to the testing of ICT

²⁴ 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.

business continuity plans,²⁵ capacity and performance management,²⁶ logging,²⁷ ICT project management,²⁸ encryption and cryptographic controls and cryptographic key management.²⁹

Of particular concern, a number of these Licence Holders failed to have in place approved capacity performance management procedures which allow for, *inter alia*, the adequate identification of capacity requirements of their ICT systems.³⁰ In addition, a number of Licence Holders have not considered, in their assessment through the testing of the ICT business continuity plans, scenarios linked to insolvency or failure of the ICT third-party service providers.³¹

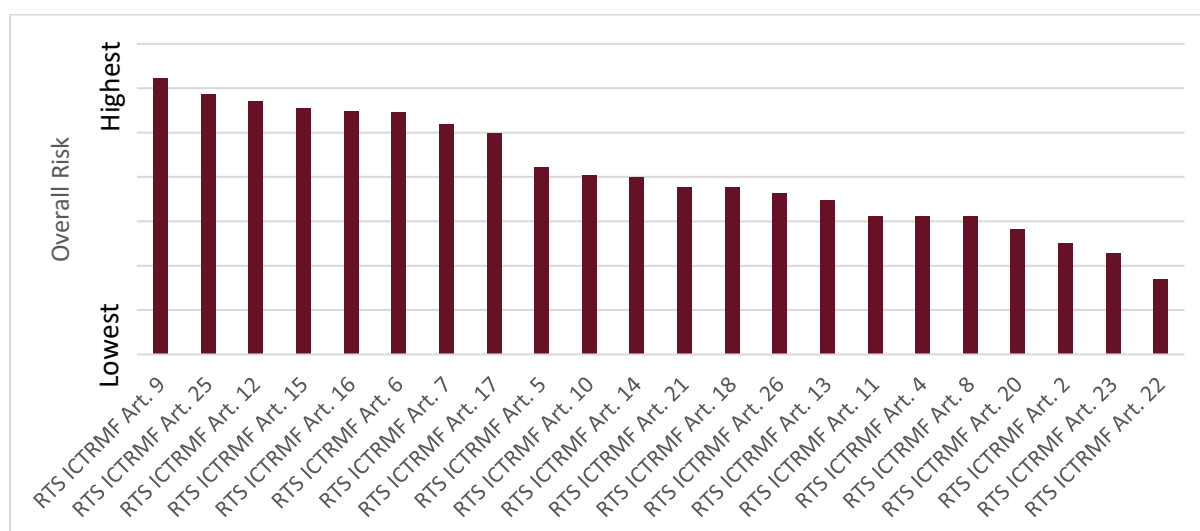


Figure 6 - Bar Chart of the Overall Risk per assessed article of the RTS ICTRMF for 2025

Overall, compliance with the RTS ICTRMF requirements remains a matter of concern, as many of those Licence Holders who have not fully achieved the assessed controls continue to demonstrate significant areas requiring improvement. Persistent weaknesses in the key areas highlighted above limit the coherence, applicability, and effectiveness, of the ICT Risk Management Framework.³² Nevertheless, in view of the progress achieved under the relevant DORA Chapters and the advancements noted since the 2024 assessment, the findings suggest that overall, the industry is moving in the right direction, though accelerated efforts will be required to achieve satisfactory regulatory compliance.

²⁵ RTS ICTRMF, art. 25.

²⁶ RTS ICTRMF, art. 9.

²⁷ RTS ICTRMF, art. 12.

²⁸ RTS ICTRMF, art. 15.

²⁹ RTS ICTRMF, arts. 6 and 7.

³⁰ RTS ICTRMF, art. 9(1).

³¹ RTS ICTRMF, arts. 25(2)(b) and 25(2) para. 3.

³² DORA, art. 6 and art. 16.

8.0 DORA Regulatory Technical Standards – ICT Third-Party Policy

The Authority has identified a number of concerns in relation to regulatory requirements stemming from the Regulatory Technical Standards on the ICT third-party service providers policy (the “RTS ICTTPP”).³³ Overall, as displayed by Figure 7, a general level of non-compliance is observed for a number of those Licence Holders who failed to fully achieve the assessed controls, particularly in relation to governance arrangements³⁴ and the required due diligence assessments.³⁵ In particular, several Licence Holders were unable to evidence that their Management Body appropriately reviews the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers on at least an annual basis, or updates it where necessary.³⁶ Furthermore, Licence Holders are experiencing difficulties in obtaining and maintaining an appropriate level of assurance over ICT third-party performance and compliance.³⁷ Another area of the RTS ICTTPP which also requires Licence Holders’ attention is in relation to the development of exit and termination strategies.³⁸

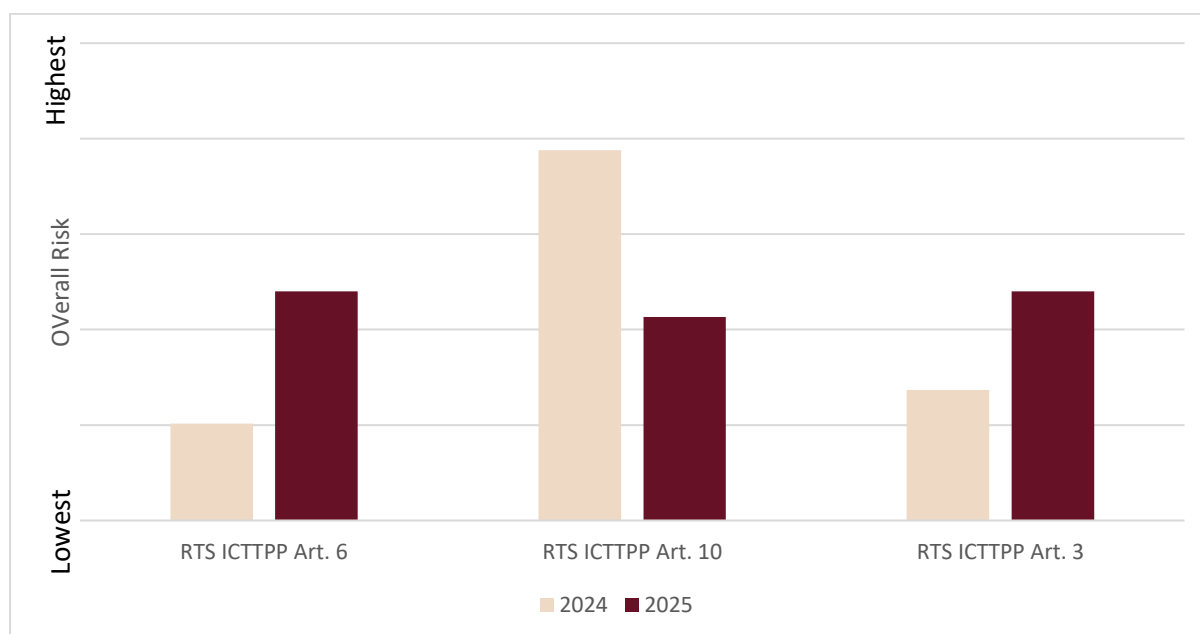


Figure 7 - Bar Chart comparing 2024 to 2025 Overall Risk per assessed article of Chapter V of DORA

³³ 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.

³⁴ RTS ICTTPP, art. 3.

³⁵ RTS ICTTPP, art. 6.

³⁶ RTS ICTTPP, art. 3(1).

³⁷ RTS ICTTPP, arts. 6(3) and 6(4).

³⁸ RTS ICTTPP, art. 10.

Overall, our data indicates that several Licence Holders must strengthen both governance and lifecycle management of ICT third-party engagements in order to meet the expectations of the RTS ICTTPP. These deficiencies significantly undermine operational resilience. Weak governance structures reduce accountability and limit the effectiveness of oversight over ICT third-party arrangements. Similarly, poor due diligence assessment impairs a Licence Holder's ability to properly assess the reliability, security standards, and risk profile of its ICT third-party providers. If left unaddressed, such shortcomings may ultimately jeopardise the continuity and security of critical functions.

9.0 Conclusion

Overall, the Authority is encouraged by the progress registered by its Licence Holders during 2025, as it is clear that the commitment towards full and satisfactory compliance with DORA and Level 2 texts is being taken seriously. When compared with the previous year's assessment, there are noticeable improvements. The Authority extends its sincere appreciation to all Licence Holders who dedicated time, effort, and expertise towards supporting the Authority's supervisory initiatives. This shared commitment is testament of the recognised need to safeguard ICT systems and maintain operational continuity within an increasingly digital financial ecosystem.

Nonetheless, the Authority acknowledges that more work remains to be done. The gaps discovered in relation to the RTS ICTRMF and RTS ICTTPP highlight a need for more in-depth day-to-day application of the risk management framework and a better understanding of the risks tied to ICT third-party service providers and how to mitigate those risks effectively. Furthermore, although DORA Chapters II to V show noticeable improvements, certain areas such as governance and organisation, cyber threat classification, and encryption and cryptographic controls remain concerning, as they continue to reveal gaps that are still unaddressed. Having emphasised this, the Authority remains committed to supporting its Licence Holders on this journey and looks forward to continued collaboration in building a digitally resilient financial system.

Further to the above and by way of the Authority's commitment to supporting its Licence Holders, the Authority has updated and published new Annex 05 and Annex 50 templates for entities wishing to obtain a licence with the Authority. These new annexes may be found under the respective Application tab for each applicable Licence type within the MFSA's Authorisations Catalogue.³⁹

³⁹ <https://www.mfsa.mt/our-work/authorisations/>

Please be guided accordingly.

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

Yours Sincerely,
Malta Financial Services Authority

Prof. Christopher Buttigieg
Chief Officer Supervision

**Christopher
P. Buttigieg**

Digitally signed by
Christopher P.
Buttigieg
Date: 2026.10.15
15:36:34 +02'00'

Mr Alan Decelis
Head Supervisory ICT Risk
and Cybersecurity

**Alan
DECELIS
(Signature)**

Digitally signed by
Alan DECELIS
(Signature)
Date: 2026.10.15
13:04:57 +02'00'

The MFSA ensures that any processing of personal data is conducted in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation), the Data Protection Act (Chapter 586 of the Laws of Malta) and any other relevant European Union and national law. For further details, you may refer to the MFSA Privacy Notice available on the MFSA webpage www.mfsa.mt.