26 September 2025

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

The Board of Directors

Re: Supervisory Engagements and Digital Operational Resilience 2024 - General Observations Report

In 2024, 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 and the Supervisory Assessments were carried out using the Authority's Risk-based Approach and Outcomes-based Supervision as detailed in the Authority's Supervision Priorities 2024. We extend our sincere appreciation for those Licence Holders who were in scope of the Authority's 2024 Supervisory Engagement Plans and committed the necessary resources to fulfil the Authority's requirements and expectations.

Outcomes-based Supervisory Engagements

In 2024, SIRC piloted the Authority's Outcomes-based, which entails a 3-year supervisory engagement cycle with a Licence Holder. The goal of this methodology is to re-engage and re-assess a Licence Holder, using the same Supervisory Engagement Tool and the same controls, two years after the initial Supervisory Engagement.[1] Whilst affording the Authorised Person a full twelve-month lead time to remediate, the Authority expects the Licence Holder in scope of Outcomes-based Supervision, to be

[1] Malta Financial Services Authority, *Supervision Priorities 2024,* pg. 16. <link>

fully aligned with all controls in two-years time, whilst ensuring that those controls which were in place at time of initial assessment, remain in place and effective.

Non-Outcomes-based Supervisory Engagements

Notwithstanding the Authority's Outcomes-based Supervision, in 2024, SIRC conducted several Supervisory Engagements which did not entail Outcomes-based Supervision. In fact, only **13%** of SIRC 2024 Supervisory Engagements were carried out using the Authority's Outcomes-based Approach, a figure which SIRC intends to increase incrementally in the coming years.

The contents of this Letter details SIRC's general observations from all 2024 Supervisory Engagements, which includes Outcomes-based Supervision and non-Outcomes-based Supervision.

Outcomes-based Supervisory General Observations

SIRC is pleased to present its general observations following the completion and analysis of data gathered through its 2024 Supervisory Engagement Plan. The Authority is encouraged by the overall findings, which indicate a strong and growing commitment across the sector to enhancing digital operational resilience, albeit areas of improvement are being recommended.

In 2024, SIRC prioritised four main areas of supervision.[2]

1. Sufficient DORA Preparedness;

[2] ibid, pg. 21.

2. Implementation of Strong Risk Management and Compliance Functions;
3. Adequate Incident Management Processes; and
4. Satisfactory Status of Third-Party Providers.

For all four outcomes in scope of SIRC 2024's Outcomes-based Supervision, 61% of all assessed controls attained a fully achieved score, 28% attained a partially achieved score, and only 9% attained not met score. These figures show that nearly 90% of all controls were either fully or partially satisfied, which is a positive outcome which demonstrates that the sector is making meaningful progress in aligning with regulatory expectations.

Despite this encouraging performance, the Authority has identified recurring areas of improvement that merit sector-wide attention. For ease of reference, these trends have been grouped according to the relevant chapters of the Digital Operational Resilience Act.[3]

DORA Chapter II – ICT Risk Management

A significant number of Licence Holders showed weaknesses in implementing robust ICT risk management frameworks. Non-compliance was frequently observed in areas such as risk identification,[4] risk mitigation,[5] and governance.[6] Additionally, several

[3] 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.

[4] DORA, arts 6(1) & 6(3).

[5] DORA, art. 6(5).

[6] DORA, art. 5(2).

Licence Holders failed to meet requirements related to third-party risk management[7] and the integration of ICT risk into the overall risk management framework.[8] These gaps suggest that while risk awareness is improving, execution and integration remain inconsistent across the sector.

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

The Authority also noted deficiencies in incident response capabilities. Many Licence Holders struggled with incident classification,[9] reporting protocols,[10] and maintaining effective communication channels during ICT disruptions.[11] These shortcomings pose a risk to operational continuity and regulatory compliance, particularly in light of the increasing frequency and complexity of cyber threats.

DORA Chapter IV – Digital Operational Resilience Testing

The Authority observed that while some Licence Holders have initiated steps toward resilience testing, many are still in the early stages of implementation. The data indicates limited evidence of structured testing programmes aligned with DORA requirements, including advanced testing such as threat-led penetration testing.[12] To

[7] 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, art. 5(2).

[8] 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, art. 2(1)(g).

[9] DORA, arts. 9(1) & 9(2).

[10] DORA, art. 13(1).

[11] n(7) art. 3(6).

[12] For example see TIBER-EU.

this extent, the Authority has recently issued its TIBER-MT Framework and encourages its Licence Holders to adopt it into its policies and procedures.[13] Several Licence Holders reported conducting security reviews such as vulnerability assessments,[14] but internal audit functions often lack the necessary ICT expertise to independently review resilience measures. Furthermore, the absence of comprehensive testing frameworks and inconsistent documentation of test results[15] suggest that resilience testing is not yet embedded as a core component of operational preparedness.

DORA Chapter V – Managing of ICT Third-party Risk

Whereas Licence Holders have initiated steps toward DORA compliance in this area, such as maintaining a register of outsourcing arrangements and beginning to align contractual provisions, some areas require further attention.

Notably, the Register of Information lacks full coverage of critical data points required,[16] and the outsourcing policy does not yet fully reflect the responsibilities and governance structures.[17] Furthermore, most Licence Holders have not yet fully implemented mechanisms to ensure that third-party providers uphold service continuity, confidentiality, and auditability.[18] The control function's oversight of outsourcing risks, including cyber risks, remains underdeveloped, and contractual provisions for exit strategies and sub-outsourcing require further refinement. These findings underscore the need for a more robust and integrated third-party risk

[13] Malta Financial Services Authority, *TIBER-MT and DORA TLPT-MT National Implementation Document*, dated 7 July 2025. <link>

[14] DORA, art. 25(1).

[15] DORA, art. 11(6)(b).

[16] DORA, art. 28(3).

[17] DORA, art. 28(1); n(7).

[18] DORA art. 30.

management framework to meet DORA's stringent requirements and ensure operational resilience across outsourced ICT services.

Non-outcomes-based Supervisory General Observations

The results from non-outcomes-based supervisory engagements are promising and reflect a positive trend. However, the slightly wider gap in performance compared to outcomes-based engagements suggests there is room for improvement. The distribution of scores, 55% fully achieved, 24% partially achieved, and 21% not met, highlights both progress and areas where further strengthening of controls is needed. Continued focus on these areas will be essential to ensure consistent supervisory standards across all engagement types.

To this extent, the Authority has identified the areas of improvement that merit sector-wide attention. For ease of reference, these trends have been grouped according to the relevant chapters of DORA.

DORA Chapter II – ICT Risk Management

The Authority observed that while many Licence Holders have made progress in developing ICT risk management frameworks, several gaps remain. Common shortcomings include inconsistent alignment with industry standards,[19] limited integration of ICT risk into broader risk management processes,[20] and insufficient documentation and review of ICT risk registers.[21] Additionally, Licence Holders often lacked robust mechanisms for identifying and mitigating risks arising from ICT third-

[19] DORA, art. 11(6)(1).

[20] DORA, art. 11(6)(4).

[21] DORA, art. 11(6)(5).

party providers,[22] and failed to fully implement change management procedures.[23] These issues suggest that while awareness is growing, further efforts are needed to embed ICT risk management into core governance structures.

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

The Authority noted persistent deficiencies in incident response capabilities across its Licence Holders. Many struggled with incident classification,[24] reporting protocols,[25] and maintaining effective communication channels during ICT disruptions.[26] Furthermore, Licence Holders often lacked comprehensive incident management procedures[27] and failed to escalate major incidents to internal and external stakeholders in a timely manner.[28] These gaps pose a risk to operational continuity and regulatory compliance, especially given the increasing complexity of cyber threats.

DORA Chapter IV – Digital Operational Resilience Testing

Findings under this chapter revealed that while some Licence Holders have initiated steps toward resilience testing, many are still in the early stages of implementation. There is limited evidence of structured testing programmes aligned with DORA requirements,[29] and a few Licence Holders have conducted advanced testing such as

[22] n(7) art. 3(6)(a).

[23] DORA, art. 9(3).

[24] DORA, arts 9(1) & 9(2).

[25] DORA, art. 13(1).

[26] n(7) art. 3(6).

[27] DORA, art. 17(1).

[28] DORA, arts 17(3)(d) and 19(1).

[29] DORA, arts 24 and 25.

threat-led penetration testing.[30] Internal audit functions often lack the necessary ICT expertise to independently review resilience measures.[31] These observations highlight the need for accelerated development of testing frameworks to ensure preparedness against evolving digital threats.

DORA Chapter V – Managing of ICT Third-party Risk

Similarly to the observations noted in the Outcomes-based Supervisory part of this Letter, the review yields that while steps have been taken, several critical areas remain partially compliant. Licence Holders have begun developing a Register of Information, but the completeness and accuracy of the register require enhancement to meet the Implementing Technical Standards.[32] Discussions with ICT third-party providers regarding DORA have commenced, yet the alignment of contractual provisions, including exit strategies, audit rights, and service continuity, remains incomplete.[33]

The outsourcing policy, though established, lacks full integration of governance responsibilities, risk assessments, and monitoring mechanisms.[34] Additionally, the control function's oversight of outsourcing arrangements and cyber risks is underdeveloped, and due diligence procedures for critical ICT services need strengthening. These gaps highlight the urgency for Licence Holders to reinforce its third-party risk management framework to ensure full compliance with DORA's operational resilience standards.

[30] Please refer to notes 12 and 13 of this Letter.

[31] DORA, art. 24(2).

[32] n(7).

[33] DORA, art. 30.

[34] DORA, arts 28(1) and 28(2).

Conclusion

Overall, the Authority is encouraged by the positive strides made by its Licence Holders in 2024, particularly the growing commitment to digital operational resilience. The progress observed, especially in the Outcomes-based Supervisory Engagements, demonstrates that many Licence Holders are actively investing in the necessary frameworks, controls, and resources to meet regulatory expectations. The Authority extends its sincere appreciation to all Licence Holders who dedicated time, effort, and expertise towards supporting the Authority's supervisory efforts. This collective momentum is a testament to the sector's recognition of the importance of safeguarding ICT systems and ensuring continuity in an increasingly digital financial ecosystem.

Nonetheless, the Authority acknowledges that more work remains to be done. Recurring gaps in ICT risk management, incident response, and resilience testing highlight the need for continued focus and improvement. Digital operational resilience is not merely a regulatory requirement. It is a fundamental pillar of trust, stability, and competitiveness in the financial sector. As cyber threats grow in frequency and sophistication, the ability to anticipate, withstand, and recover from ICT-related disruptions becomes ever more critical. 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.

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

Supervisory ICT Risk and Cybersecurity function

Mr Alan Decelis
Head

Alan DECELIS (Signature)
Digitally signed by Alan DECELIS (Signature)
Date: 2025.09.26 13:04:21 +02'00'

Mr Christopher Aquilina
Deputy Head

Christopher AQUILINA (Signature)
Digitally signed by Christopher AQUILINA (Signature)
Date: 2025.09.26 09:39:13 +02'00'

MFSA MALTA FINANCIAL SERVICES AUTHORITY

We are excited to announce the launch of the **Cyber Finance Summit**, a milestone event that will highlight Malta's commitment to reinforcing its position as a leading hub for cybersecurity dialogue in the financial services sector.

The summit will take place on 15 and 16 October at MCC, Valletta, Malta.

During the event, we will be welcoming experts from Europe and beyond: Industry professionals, financial entities, ICT third-party service providers and regulators will be brought together to encourage collaboration and share knowledge on cybersecurity and digital operational resilience.

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

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

WHAT TO EXPECT

- **Keynote Presentations** from Industry Experts
- **Panel Discussions** on Cutting-Edge Topics
- **Networking Opportunities** with Key Stakeholders

FEATURED TOPICS

- Financial Supervision in the Digital Age
- Evolving Cyber Threat Landscape
- Macro-Prudential Cyber Resilience Approaches
- Latest Regulatory Developments
- ICT Third-Party Risk Management
- Supply Chain Security
- Emerging Technologies and Their Implications

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

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

REGISTRATION

The Authority encourages interested participants to register by not later than **16 October 2025**.

Participants who attend will be eligible for CPD hours.

Photos and videos will be taken during the event with the intent to publish such on social media channels and website. By registering, one would be granting consent to such data being used.

REGISTER NOW

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

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