MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

5 August 2026

Frontier Artificial Intelligence Models and the Evolving Cyber-Threat Landscape

This Circular applies to all Licence Holders. References to Regulation (EU) 2022/2554 on digital operational resilience for the financial sector ("DORA") apply only to those Licence Holders falling within its scope.

Background and Recent Developments

The Malta Financial Services Authority (the "MFSA" or the "Authority") draws Licence Holders' attention to recent European publications concerning the evolving cyber risks associated with Frontier Artificial Intelligence Models ("FAIMs"). These include the Warning and accompanying report issued by the European Systemic Risk Board ("ESRB"), the communication issued by European Central Bank ("ECB") and the Joint Statement published by the European Supervisory Authorities ("ESAs").

FAIMs are advanced artificial intelligence ("AI") models with capabilities that may materially affect offensive and defensive cyber operations. The European publications indicate that such models may enable cyber activity to be conducted with greater speed and sophistication, including through the accelerated discovery of vulnerabilities and development of exploits. Although FAIMs may also support defensive capabilities, their development represents a material change in the cyber-threat landscape.

The Authority is not, through this Circular, introducing a separate set of supervisory expectations specifically addressing FAIMs. Rather, the developments highlighted by the European authorities reinforce the continued relevance of existing regulatory requirements and of the governance, risk management and prudential principles previously communicated by the MFSA, including through its Dear CEO Letter on Artificial Intelligence issued on 4 June 2026.

Implications for the Financial Sector

The Authority's Dear CEO Letter, entitled *Artificial Intelligence (AI) – Governance, Risk and Prudential Expectations*, identified AI as a prudentially relevant risk area and highlighted the importance of a forward-looking approach to governance and oversight, third-party dependencies and concentration risk, model risk, data governance, operational resilience and potential systemic implications.

While the Dear CEO Letter primarily considered risks arising from the adoption and use of AI by Licence Holders, the recent European publications highlight a related external threat dimension: the potential use of increasingly capable AI models by threat actors against financial institutions, financial infrastructure and technology providers. These two perspectives should be considered together within Licence Holders' existing governance, risk management and operational resilience arrangements.

Of particular relevance is the potential compression of the period between vulnerability discovery and exploitation. The ESRB has highlighted that FAIMs may accelerate the discovery of vulnerabilities and the development and weaponisation of exploits. This could reduce the time available to identify, prioritise, patch and otherwise mitigate vulnerabilities, placing established vulnerability-management and cyber-defence cycles under increasing pressure.

These developments do not necessarily require the creation of a separate category of "FAIM controls". They do, however, reinforce the importance of considering whether existing ICT risk management and operational resilience arrangements remain sufficiently effective in the changing threat environment. Relevant areas include asset visibility, vulnerability and patch management, security monitoring, incident detection and response, defence-in-depth, recovery capabilities and digital operational resilience testing.

Licence Holders are encouraged to consider these developments proportionately and on a risk-based basis, taking account of their size, business model, ICT architecture, critical functions, threat exposure and reliance on third-party service providers.

Third-party dependencies and concentration risk are particularly relevant. Licence Holders may rely on common cloud, technology, software, AI model and data providers, as well as other critical ICT third parties. Such dependencies may give rise to shared vulnerabilities and single points of failure, particularly where multiple entities rely on the same infrastructure, provider, model or data source.

Existing Regulatory and Supervisory Framework

For Licence Holders falling within its scope, DORA remains the regulatory anchor for digital operational resilience. The changing threat landscape increases the importance of its effective implementation, particularly in relation to ICT risk management, ICT-related incident management, digital operational resilience testing and ICT third-party risk management.

Licence Holders are encouraged to consider FAIM-related developments within their existing ICT risk management and operational resilience frameworks rather than as a separate compliance exercise. The communication issued by ECB Banking Supervision, while addressed to significant institutions under its direct supervision, also provides relevant considerations for the wider financial sector regarding the continued effectiveness of existing ICT resilience measures in an accelerating threat environment.

The technical nature of FAIM-related cyber risks does not transfer responsibility exclusively to ICT or cybersecurity functions. Management bodies should remain appropriately informed of material developments in the threat landscape and satisfy themselves that ICT risk management and operational resilience arrangements remain commensurate with the Licence Holder's risk profile, operating environment and dependencies.

The Joint ESA Statement groups relevant risk-mitigation measures into three broad areas:

1. **Prevention**, aimed at reducing the likelihood and impact of successful attacks;
2. **Detection**, aimed at identifying emerging threats, vulnerabilities and malicious activity and
3. **Management**, aimed at responding to incidents and limiting their consequences.

Licence Holders are encouraged to familiarise themselves with the measures described in the Joint ESA Statement and consider their relevance within existing risk management arrangements. The **Prevent, Detect and Manage** structure should be understood as a useful means of considering the effectiveness of existing arrangements.

The Authority may consider these developments as part of its ongoing supervision concerning ICT risk, cybersecurity, digital operational resilience, third-party risk and AI governance.

The European developments mentioned above reinforce the continued relevance and increasing urgency of existing governance, ICT risk management and operational resilience principles. Licence Holders are encouraged to consider these developments together with

the principles previously communicated by the Authority and, where applicable, their obligations under DORA.

Licence Holders may request further information by contacting sirc@mfsa.mt.