EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Digital Society, Trust and Cybersecurity
**Acting Director**

Brussels
CNECT.H.1

**NOTE FOR THE ATTENTION OF JUHAN LEPASSAAR,**
**EXECUTIVE DIRECTOR OF THE**
**EU AGENCY FOR CYBERSECURITY (ENISA)**

**Subject: Request for the preparation of a candidate Managed Security Services certification scheme under Article 48(1) of Regulation (EU) 2019/881 (Cybersecurity Act)**

Pursuant to Article 48(1) of the Cybersecurity Act (CSA), the European Commission hereby requests ENISA to prepare a candidate European cybersecurity certification scheme applicable to Managed Security Services (MSS).

*Background*

In line with Article 47 of the CSA, the European Commission published on 7 February 2024 a Union rolling work programme (URWP), which identified the strategic priorities for future European cybersecurity certification schemes. The URWP highlights MSS as a particularly relevant area for future European cybersecurity certification, noting its role in the proposal for the Cyber Solidarity Act, Regulation (EU) 2025/38 (CSoA), which entered into force on 4 February 2025.

The cyber threat landscape within the Union is becoming increasingly complex due to rapid technological advancements and the growing sophistication of cyberattacks. In response to these evolving threats, organisations are increasingly relying on Managed Security Service Providers (MSSPs) who have gained importance in the prevention and mitigation of cybersecurity incidents by delivering specialised cybersecurity expertise and operational support. While the outsourcing of security functions to MSSPs offers significant benefits, such as improved operational efficiency and access to advanced security capabilities, it also introduces notable risks. These risks primarily arise from the concentration of sensitive data and critical security responsibilities within MSSPs, making them attractive targets for malicious actors given their essential role in safeguarding the digital environments of multiple clients.

Furthermore, the CSoA provides that trusted managed security service providers need to be certified in accordance with the MSS scheme two years after the scheme is in place, in order to be part of the EU Cybersecurity Reserve, emphasising the need for the

Commission to request ENISA to prepare a candidate European cybersecurity certification scheme for MSS in the areas covered by the EU Cybersecurity Reserve.

Finally, some Member States have already created national schemes intended to certify the provision of specific MSS. To prevent an increasing risk of fragmentation of the internal market with regard to cybersecurity certification schemes in the Union, a need for a European cybersecurity certification scheme for MSS is apparent.

*Legal Framework*

To address these risks and strengthen the overall level of cybersecurity within the Union, the CSA sets up a framework for the establishment of European certification schemes. With Regulation (EU) 2025/37, the CSA was amended to enable the future adoption of European certification schemes for MSS.

The definition of MSS under the CSA includes a non-exhaustive list of MSS that could qualify for European cybersecurity certification schemes, such as incident management, penetration testing, security audits, and consulting related to technical support. MSS could encompass cybersecurity services that support the preparedness for, prevention, detection, analysis and mitigation of, response to, and recovery from incidents. Cyber threat intelligence provision and risk assessment related to technical support could also qualify as MSS. It is clarified that there could be separate European cybersecurity certification schemes for different MSS.

It is important to note that this certification framework applies specifically to the services provided by MSSPs, rather than to MSSPs as organisational entities, which are already subject to cybersecurity obligations under the Directive (EU) 2022/2555 (NIS 2 Directive). In accordance with Article 21(5), first subparagraph of the NIS 2 Directive, the Commission Implementing Regulation (EU) 2024/2690 was adopted on 17 October 2024 to ensure the consistent application of these obligations across Member States as regards certain types of entities, including MSSPs. The technical and methodological requirements for cybersecurity risk-management measures applicable to MSSPs are outlined in the Annex of the implementing regulation. Therefore, the implementing regulation provides comprehensive requirements to MSSPs on implementing cybersecurity risk-management practices and it promotes a harmonised approach across the Union, while in accordance with Article 26(1)(b) of the NIS 2 Directive, jurisdiction remains with the Member State where the MSSP has its main establishment.

For ICT third-party service providers that are critical for the EU financial sector, additional recommendations are laid down under Regulation (EU) 2022/2554 (Digital Operational Resilience Act – DORA), which establishes a comprehensive framework aimed at ensuring the operational resilience of financial entities against cyber threats. When designated as critical ICT third-party service providers in accordance with Article 31 DORA, MSSPs providing services to financial institutions are subject to the Oversight Framework established under DORA.

Moreover, the CSoA establishes the EU Cybersecurity Reserve, designed to support Member States' cyber crisis management authorities and Computer Security Incident Response Teams (CSIRTs), the CERT-EU and other competent authorities in responding to and recovering from significant and large-scale cybersecurity incidents. The EU Cybersecurity Reserve will rely on trusted MSSPs to deliver critical response services during major cyber crises. Importantly, MSS certification will be one of the procurement criteria and requirements for the trusted providers forming the EU Cybersecurity Reserve. This ensures that only MSSPs meeting the highest security, quality and operational resilience standards are entrusted with such vital responsibilities.

*Scope and Structure of the candidate MSS certification scheme*

The MSS certification framework should establish a harmonised set of service-oriented requirements designed to complement those technical, operational and organisational obligations which are placed on MSSP under the NIS 2 Directive and DORA to ensure the robustness of MSSPs as organisations. It should be structured around two distinct layers, providing a comprehensive and coherent approach to MSS delivery. These layers should consist of a horizontal layer with baseline requirements, which apply to all MSS, and vertical service pillars (or verticals), which introduce specific technical requirements tailored to individual MSS. It should be ensured that the horizontal layer is not designed as a stand-alone basis for certification.

The horizontal layer should provide one common set of baseline requirements to ensure the security, reliability and operational resilience of MSS delivered within the Union. It should thus define baseline requirements – which apply as a prerequisite and regardless the assurance levels of all vertical service pillars – in the domains of secure service and platform design, deployment and transition management, availability and continuity management, operational service management, as well as continuous improvement and technology maintenance ensuring that MSS technologies remain secure and fit for purpose. These requirements should ensure that MSS are designed and implemented in a secure manner, integrated seamlessly into operational client environments, that they remain resilient against disruptions, and are effectively managed throughout their lifecycle.

Building on this common foundation established by the horizontal layer, the MSS certification framework should introduce vertical service pillars, that should constitute annexes to the horizontal layer, which define service-specific technical requirements tailored to the unique nature, operational demands and security challenges associated with specific MSS domains. Each vertical should complement the horizontal layer by setting out precise criteria, where necessary, to address the distinctive characteristics and risk profiles of the specific MSS. The use of verticals would allow for the flexibility and adaptability needed to ensure that the MSS certification framework remains relevant and responsive as the cybersecurity threat landscape continues to evolve. Through service-specific requirements, the framework can effectively address the diverse range of MSS offerings while maintaining a consistent service-focused baseline across all services.

To reflect the varying levels of compliance with different service pillars, the labels or certificates issued under this framework should be distinct and MSS-specific. Certification should clearly indicate the specific MSS for which an MSSP has demonstrated compliance with both the horizontal requirements and the relevant vertical pillar(s). This approach ensures transparency for clients and stakeholders, enabling them to easily identify the scope and coverage of an MSSPs certification.

The first vertical to be developed under the certification framework should focus on incident management, a critical function within the cybersecurity landscape and also of high priority in view of the needs for the establishment of the EU Cybersecurity Reserve under the CSoA. This vertical will cover the entire incident management lifecycle, from identification and detection through to response, recovery, and post-incident review. It should establish detailed requirements to ensure the quality, effectiveness, and security of incident management services, including processes for incident reporting, escalation procedures, coordination with relevant stakeholders and mechanisms for continuous improvement based on lessons learned from past incidents. The overarching goal is to enhance the resilience of organisations in managing and recovering from cybersecurity incidents efficiently, minimising potential disruptions and mitigating the impact of security breaches.

*Timeline*

Given the importance of the implementation of the CSoA, the development of the candidate scheme applicable to MSS should start immediately and the necessary resources should be allocated as a matter of priority. Following this request, it is suggested to aim for delivering a candidate scheme composed of the horizontal layer and the first vertical by the beginning of 2026. Once established, providers participating in the EU Cybersecurity Reserve must obtain certification under the MSS scheme within two years of its application. This ensures that all trusted MSSPs meet standardised security and quality benchmarks, reinforcing their ability to effectively support incident management.

I am grateful for ENISA's commitment, and the valuable input provided through the feasibility study, which offered important context for this request and the next steps at technical level. We are looking forward to working closely with your team towards the development of the MSS certification scheme

Christiane KIRKETERP DE VIRON

c.c.: S. Schuster, R. Stefanuc, A. Wawrzyk, I. Lauringson, A. Nevado, F. Weprajetzky