Council of the European Union
General Secretariat

Interinstitutional files:
2023/0108 (COD)

Brussels, 23 February 2024

WK 2827/2024 REV 1

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on cyber issues (attachés)
N° prev. doc.:	WK 15991/2023
N° Cion doc.:	8511/23
Subject:	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services - compromise proposals

Delegations will find in the Annex the compromise proposals related to the above legislative proposal, as result from the technical meeting held on 22 February 2024.

Compromise Package on CSA+

1. Definition for MSSP

Line 27 Article 1 (2)(b) Amending CSA article 2 (14a)

'managed security service' means a service ***provided to a third party*** consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, ***such as*** incident ***handling,*** penetration testing, security audits and ***consulting including expert advice related to technical support'***

Line 12 - Recital 2

Managed security services ***are services provided by managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 of the European Parliament and of the Council[1]. Therefore, the definition of managed security services in this Regulation should be consistent with the one of managed security service providers in Directive (EU) 2022/2555. These services*** consist of carrying out, or providing assistance for activities relating to their customers' cybersecurity risk management, ***and*** have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Accordingly, the providers of those services are considered as essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555. Pursuant to Recital 86 of that Directive, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. Essential and important entities within the meaning of Directive (EU) 2022/2555 should therefore exercise increased diligence in selecting a managed security service provider.

(new) Recital 2a

The definition of managed security services under this Regulation includes a non-exhaustive list of managed security services that could qualify for certification schemes, such as incident handling, penetration testing, security audits, and consulting, related to technical support. Managed security services could encompass cybersecurity services that support the preparedness, prevention, detection, analysis, mitigation, response to, and recovery from cybersecurity incidents. Cyber threat intelligence provision, real time threat monitoring and risk assessment might also qualify as managed security services. There may be separate European cybersecurity certification schemes for different managed security services. The European cybersecurity certificates issued in accordance with such schemes should refer to specific managed security services of a specific provider of these services.

2. Compromises on transparency, consultation and information

Amending Article 49 of the CSA

3. When preparing a candidate scheme, ENISA shall consult all relevant stakeholders ***in a timely manner*** by means of a formal, open, transparent and inclusive consultation process. ***When transmitting the candidate scheme to the Commission, as per Article 49(6), ENISA shall provide information on how it has complied with this obligation.***

4. For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise.

The ad-hoc working groups established for this purpose shall, as appropriate and without prejudice to the procedures and discretion established by Article 20(4), include experts from the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector.

New Article 49A to the CSA

Information and consultation on the European cybersecurity certification schemes

1. The Commission shall make the information on its request to ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme referred to in Article 48 publicly available.

2. During the preparation of a candidate scheme by ENISA in line with Article 49, the European Parliament as well as the Council may request the Commission in its capacity as chair of the European Cybersecurity Certification Group (ECCG) and ENISA to present relevant information on a draft candidate scheme on a quarterly basis. Upon the request of the European Parliament or the Council, ENISA, in agreement with the Commission, and without prejudice to Article 27, may make available to the European Parliament and to the Council relevant parts of a draft candidate scheme in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner.

3. In order to enhance the dialogue between the Union institutions and to contribute to a formal, open, transparent and inclusive consultation process, the European Parliament as well as the Council may invite the Commission and ENISA to discuss matters concerning the functioning of European cybersecurity certification schemes for ICT products, ICT services, ICT processes or managed security services.

4. The Commission shall take into account, where appropriate, elements arising from the views expressed by the European Parliament and the Council on the matters referred to in paragraph 3 of this Article when evaluating this Regulation in line with Article 67.

(new) Recital xxx

This Regulation provides for targeted amendments to Regulation 2019/881 to add the possibility to create cybersecurity certification schemes for managed security service providers. In doing so, it should also specify or clarify certain provisions concerning the preparation and functioning of all European cybersecurity certification schemes with a view to ensuring their transparency and openness. The latter amendments, which are limited to specification or clarification of Regulation 2019/881, should not prejudge in any way the broader evaluation and review of that Regulation required under its Article 67, including specifically the evaluation of the impact, effectiveness and efficiency of that Regulation's Title relating to cybersecurity certification schemes.

3. Outcomes from the previous CSA+ trilogue on 4/12/2023

➔ **Recital on Skills**

Recital 5c)

The Union is faced with a talent gap, characterised by a shortage of skilled professionals, and a rapidly evolving threat landscape as acknowledged in the Commission communication of 18 April 2023 on the Cybersecurity Skills Academy. Educational resources and forms of formal training differ and knowledge can be acquired in various ways, both formal, for example through university or courses, and informal, for example through on-the-job training or work experience in the relevant field.

Therefore, in order to facilitate the emergence of high-quality, essential managed security services and to have a better overview of the composition of the Union cybersecurity workforce, it is important that cooperation between Member States, the Commission, ENISA and stakeholders, including the private sector and academia, is strengthened through the development of public-private partnerships, support of research and innovation initiatives, the development and mutual recognition of common standards and certification of cybersecurity skills, including through the European Cyber Security Skills Framework. Such cooperation would also facilitate the mobility of cybersecurity professionals within the Union as well as the integration of cybersecurity knowledge and training in educational programmes, while ensuring access to apprenticeships and traineeships for young people, including persons living in disadvantaged regions, such as islands, sparsely populated, rural and remote areas. It is important that those measures aim to attract more women and girls in the field and contribute towards addressing the gender gap in science, technology, engineering, and mathematics, and that the private sector aims to deliver on-the-job training addressing the most in-demand skills, involving public administration and start-ups, as well as microenterprises and SMEs. It is also important that the providers and Member States collaborate and contribute to the collection of data on the situation and the evolution of the cybersecurity labour market.

➔ **Recital on ENISA (in line with CRA line 71a)**

Recital 5d)

ENISA plays an important role in the preparation of European certification candidate schemes. The Commission should assess the necessary budgetary resources for ENISA's establishment plan, in accordance with the procedure set out in Article 29 of Regulation (EU) 2019/881 when preparing the draft general budget of the Union.