European Union Agency for Cybersecurity
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711 | e-mail: info@enisa.europa.eu
www.enisa.europa.eu

CALL FOR APPLICATIONS: ENISA'S AD-HOC WORKING GROUP ON MANAGED SECURITY SERVICES CERTIFICATION

1. INTRODUCTION

Managed Security Services (MSS) have emerged as a vital component of modern cybersecurity ecosystems, in which Managed Security Service Providers (MSSPs) carry out, or provide 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.[1] These services play a pivotal role in supporting the cybersecurity risk management strategies of client organisations and are increasingly recognised as essential in preventing and mitigating cyber incidents.

Recognising the strategic importance of MSS in strengthening Europe's cybersecurity posture, the Union Rolling Work Programme, published in January 2024, identified MSS as a key priority for the development of a future EU cybersecurity certification scheme. This priority was further solidified through the amendment of the Cybersecurity Act (CSA), adopted on 4 February 2024, which explicitly incorporates provisions for the certification of MSS.[2] In response, ENISA initiated a feasibility study and market analysis to assess the current state of the MSS landscape and to identify the technical, operational, and regulatory elements that will inform the development of a future certification scheme.

Following the request from the European Commission to establish a certification scheme on MSS, ENISA now intends to establish a dedicated Ad Hoc Working Group (AHWG) to support the Agency in preparing a candidate European cybersecurity certification scheme for MSS (EUMSS). This expert group will convene leading professionals from across the cybersecurity ecosystem to provide structured input on the scope of the scheme, assurance levels, applicable standards, conformity assessment mechanisms, and related policy and implementation considerations. To this end, ENISA is launching this call for applications to select qualified members of the AHWG. Selected experts will play a vital role in shaping a certification scheme that is both technically robust and strategically aligned with EU policy goals, ensuring that MSS offered across the Union are secure, reliable, and meet the evolving needs of the Internal Market

[1] Directive (EU) 2022/2555
[2] Consolidated text : Regulation (EU) 2019/881

2. BACKGROUND OF THE AD HOC WORKING GROUP

As set out in Regulation (EU) 2019/881 (hereafter: "the Cybersecurity Act"), the EU cybersecurity certification framework establishes the procedure for developing European cybersecurity certification schemes for ICT products, services, and processes.[3] Each scheme can define one or more assurance levels – basic, substantial, or high – based on the risk associated with the intended use of the product, service, or process. ENISA is responsible for preparing candidate schemes that meet the criteria specified in Articles 51, 52, and 54 of the Cybersecurity Act, following a request from the European Commission or, in certain cases, from the European Cybersecurity Certification Group (ECCG).[4]

To support the preparation of such schemes, the Cybersecurity Act provides for the creation of ad hoc working groups (AHWGs) composed of subject-matter experts. Specifically, for each candidate European cybersecurity certification scheme, ENISA must establish an AHWG to provide specific advice and expertise.[5] The establishment of such group shall be subject to the provisions set out in Article 20(4) of the Cybersecurity Act, which stipulates that '*where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad-hoc working groups composed of experts, including experts from the Member States' competent authorities*. The Management Board must be informed prior to the establishment of any such group.[6] The modalities for establishing and operating AHWGs are detailed in ENISA Management Board Decision No MB/2022/5. In accordance with Article 2 of this Decision, these groups are established through open calls for expressions of interest and are tasked with supporting ENISA in fulfilling specific objectives and tasks under the Cybersecurity Act.[7]

The Management Board has been informed by ENISA in its meeting on 17 June 2025 and consequently, ENISA is launching this call for expression of interest to establish an AHWG to support the development of EUMSS under Activity 7 of the Single Programming Document 2025-2027 (SPD). The AHWG will provide their expertise in the scheme's development, most notably on the elements of the candidate scheme in accordance with Article 54 of the CSA, such as scope, purpose assurance levels, etc.

[3] Consolidated text: Regulation (EU) 2019/881
[4] Articles 48 and 49 of Regulation (EU) 2019/881.
[5] Article 49(4) of Regulation (EU) 2019/881.
[6] Article 20(4) of Regulation (EU) 2019/881.
[7] Decision No MB/2022/5 of the Management Board of the European Union Agency for Cybersecurity (ENISA) on the establishment and operation of ad hoc working groups and repealing MB Decisions No MB/2013/11 and No MB/2019/11. Available online at: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2022-05-on-ad-hoc-working-groups.pdf.

3. SCOPE OF THE AD HOC WORKING GROUP

3.1 SCOPE OF WORK

In accordance with Article 48(1) of Regulation (EU) 2019/881, the European Commission has requested ENISA to develop a candidate EUMSS. In line with the European Commission's request, the scheme should aim to define a harmonised set of service-oriented requirements that complement the technical, operational, and organisational obligations imposed on MSSPs under the NIS 2 Directive and DORA. This certification framework should apply specifically to the services provided by MSSPs, rather than to MSSPs as organisational entities. Considering this, the framework will consist of two layers:

- **Horizontal Layer**: Applies to all MSS and defines a common set of baseline requirements in areas such as secure service and platform design, deployment and transition management, availability and continuity management, operational service management, continuous improvement and technology maintenance. These common requirements aim to ensure the security, reliability, and resilience of MSS across the EU.
- **Vertical Layers**: These introduce service-specific technical requirements tailored to particular MSS service domains. They complement the horizontal layer to address domain-specific operational and security needs, allowing the framework to remain adaptable to evolving threats.

The first vertical to be developed should focus on incident management, commencing with a targeted approach on incident response as part of a gradual approach that will eventually and progressively cover the full incident management lifecycle — from detection through recovery to post-incident review. The vertical will aim to define detailed requirements to ensure the quality, effectiveness, and security of incident management services. The overarching objective is to strengthen organisational resilience by enabling timely and efficient management of cybersecurity incidents, minimising disruption, and reducing the impact of security breaches.

This work is closely aligned with the objectives of Regulation (EU) 2025/38 (hereafter: "Cyber Solidarity Act" of "CSoA'),[8] which seeks to strengthen the EU's collective cybersecurity posture through enhanced preparedness, coordinated response capabilities, and cross-border cooperation. Under this framework, a Cyber Reserve is being established which shall consist of a pool of trusted and certified cybersecurity service providers that can be deployed to support Member States and critical sectors in the event of large-scale cyber incidents. In accordance with the European Commission's 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 (2) years of its application.

[8] Regulation (EU) 2025/38

3.2 WORKING GROUP DURATION AND ACTIVITIES

The working group will be established for up to four (4) calendar years from the date of the Agency Decision launching its operations. The mandate may be extended if the scope of work is not completed within this timeframe.

Interaction frequency will be coordinated between ENISA and the group members. Members, including those on the reserve list, may be called upon for additional tasks, subject to remuneration as per Section 8.2 of the Call.

Non-exhaustive list of typical activities that the members of this AHWG might undertake:

- Drafting and reviewing common horizontal criteria for MSS.
- Identifying domain-specific requirements for vertical service pillars.
- Providing expert input on incident management processes and standards.
- Supporting public consultations and refining scheme deliverables.
- Analysing alignment with existing EU legislation (NIS 2, DORA, CSoA), in close cooperation with the European Commission.
- Contributing to the design of assurance levels and evaluation methods.

4. SELECTION AND APPOINTMENT OF MEMBERS AND OBSERVERS

4.1 CONDITIONS FOR MEMBERS

Composition: The membership of the AHWG will be composed of up to 30 leading experts selected through this open call, based on the requirements and competencies outlined. These members will bring together a balanced mix of horizontal and vertical expertise relevant to the certification of MSS.

In forming the group, ENISA will consider a range of factors to ensure a representative and effective composition. This includes geographical diversity, gender balance, and a well-rounded representation of key stakeholder groups. These stakeholders span both the supply side – such as MSS technology vendors, integrators, and service operators – and the demand side, including end-users of MSS, critical infrastructure and public entities. Stakeholders from the conformity assessment community (including CABs, auditors, certification bodies, and testing laboratories) and academic experts with deep knowledge of network and information security will also be considered.

Reserve List: If the number of suitable applicants exceeds the required number of members for the Ad Hoc Working Group (AHWG), ENISA will establish a reserve list of individuals. While an initial cohort of up to 30 members will be appointed to the AHWG, ENISA reserves the right to draw from the reserve list at any time should additional expertise be required to support the group's mandate.

Reserve list members may be called upon under the same terms and conditions as appointed members, particularly to replace individuals who are unavailable, disqualified, have resigned, or are otherwise unable to fulfil their duties. If an appointed member informs the Chairperson that they can no longer actively contribute to the AHWG, the Chairperson may—upon the member's request—place them on the reserve list for potential future re-engagement.

Appointment: Members of the AHWG will be appointed *ad personam* by the Executive Director of ENISA from a list of suitable experts selected through this open call. Appointed members shall serve in their personal capacity, acting independently and in the public interest, without directly representing any organisation or stakeholder group.

While appointment is strictly personal, appointed members are encouraged to suggest suitable alternatives from within their organisation who may temporarily contribute to the work of the AHWG during their absence, subject to the Chairperson's approval and the operational requirements of the AHWG. These suggestions do not imply formal appointment but can help maintain continuity in the group's output.

Replacement: Should a member no longer be able to contribute effectively to the work of the AHWG, fail to comply with the conditions set out in Article 339 of the Treaty on the Functioning of the European Union, resign, or otherwise become unavailable, their participation in the group will be discontinued. In such cases, ENISA may appoint a replacement from the established reserve list to serve for the remainder of the AHWG's term. Additionally, if a member voluntarily notifies the Chairperson that they can no longer fulfil their duties, the Chair may, upon the member's request, place them on the reserve list.

4.2 CONDITIONS FOR OBSERVERS

Permanent observers may include a range of organisations with public-interest missions, such as national regulatory bodies, sectoral associations, academic consortia, and other stakeholders serving a broader public goal. These entities may apply for observer status as described in the section 9 of this call, and are required to submit an application in accordance with Section 9.2 of this call.

Certain categories of observers may participate in the activities of the AHWG without undergoing a formal selection procedure. These include:

- Representatives of EU Institutions, bodies, offices, and agencies (EUIBAs);
- Public authorities of Member States and EEA/EFTA countries;
- European and international standardisation bodies;
- International Organisations with a relevant mandate.

These participants serve as observers who may participate in the activities of the AHWG, but are not considered appointed members of the AHWG. Accordingly, they are not eligible for reimbursement of expenses under the provisions outlined in Section 8 of this call.

5. ORGANISATION OF THE AD HOC WORKING GROUP

5.1 SECRETARIAT AND RULES OF PROCEDURE

Chairperson. The Chairperson of the AHWG will be designated by the Executive Director of ENISA from among ENISA staff. Where deemed appropriate and based on the operational needs of the AHWG, the Chairperson may appoint up to two Vice-Chairpersons from ENISA staff.

The Chairperson shall be responsible for convening meetings, managing the agenda, coordinating the timely distribution of relevant information and documents, and addressing all organisational matters to ensure the effective operation of the AHWG. Meeting agendas will be distributed no later than four (4) working days prior to each meeting of the AHWG. ENISA will provide the Secretariat to support the functioning of the AHWG.

Rules of Procedure: At the start of the AHWG, the Chairperson will present a draft set of Rules of Procedure (RoP) outlining the AHWG's framework, roles, responsibilities, and decision-making processes. These rules will cover key aspects such as meeting formats and frequency, confidentiality obligations, conflict of interest provisions, voting procedures (where applicable), reporting lines, and mechanisms for resolving disagreements.

The draft RoP will be submitted to the AHWG members for review and adopted by consensus or majority agreement, as appropriate. Once adopted, the RoP will serve as the governance structure guiding the AHWG's functioning throughout its mandate. ENISA may propose revisions to the rules, subject to the group's approval, to accommodate evolving needs or ensure alignment with regulatory and strategic priorities.

5.2 THEMATIC GROUPS

Taking into account the modular structure of the EUMSS framework, the Chairperson may decide to establish Thematic Groups within the AHWG, each corresponding to specific MSS verticals or areas of work to be addressed. If such Thematic Groups are established during the course of the AHWG's activities, members will be invited to participate based on their expertise, professional background, and expressed interest in the relevant domain. ENISA will ensure adequate cooperation and the effective exchange of information between these groups. This approach promotes focused contributions, enables in-depth discussion within specialised areas, and supports a flexible and scalable working model aligned with the evolving scope of MSS certification.

5.3 ORGANISATIONAL MODALITIES

The AHWG will primarily convene remotely, with meetings held online, at ENISA premises in Athens or Brussels, or at other locations as proposed by the Chairperson. The majority of the group's work will be conducted virtually, and the use of secure video or teleconferencing is encouraged to facilitate collaboration and ongoing exchanges among members of the AHWG.

ENISA will convene plenary sessions of the full AHWG at least four (4) times per calendar year. Additional meetings may be organised more frequently for Thematic Groups established to support dedicated work streams.

6. CONFIDENTIALITY AND DECLARATIONS OF INTEREST

Confidentiality: Members of the AHWG – including invited experts and observers – are bound by the obligation of professional confidentiality as set out in Article 27 of Regulation (EU) 2019/881.They must comply with the confidentiality provisions of Article 339 of the Treaty on the Functioning of the European Union (TFEU), which continue to apply even after their involvement with the group has ended. Prior to the first meeting of the AHWG, each member is required to submit a signed confidentiality declaration in writing.

Security Clearance: ENISA will comply with Commission Decision (EU, Euratom) 2015/444 on the protection of EU classified information. While a valid security clearance is not required to apply to the AHWG, ENISA may request appointed members to obtain a security clearance from their national authorities if the group's work would come to involve restricted or classified information. The responsibility to commence and complete this process will fall solely on the individual member. ENISA will not facilitate, mediate, or intervene in clearance procedures with national authorities on behalf of AHWG members.

Access to Documents: Members of the AHWG – including invited experts and observers – are subject to the provisions of Regulation (EC) No 1049/2001 on access to documents.[9]

Information Sharing: While Members – including invited experts and observers – may consult with their organisations or relevant external parties as needed for their work in the AHWG, such exchanges must be limited to a need-to-know basis. Information that is explicitly marked as confidential – either in writing or by the Chair or Vice-Chair of the AHWG – must not be disclosed under any circumstance. Any information produced by the AHWG may only be made public with the prior approval of the Chair.

Public Disclosure: Once ENISA has officially published the list of appointed AHWG members, individuals may publicly disclose their membership and refer to the general scope and objectives of the AHWG's work.

Declarations of interest: The members of the AHWG are subject to the obligations of Article 25 (2) of Regulation (EU) 2019/881. Before the start of the first meeting, each member shall declare in writing, that if there are any interests that might be considered to be prejudicial to their independence in relation to the items on the agenda, he or she shall abstain from participating in the discussion of and voting on such items. This applies only to the topic of the agenda meaning that (additional) participants/AHWG members can fully participate in the meeting related to the remaining topics.

In accordance with Article 26(2) of Regulation (EU) 2019/881, the signed declarations of interest submitted by AHWG members must be made publicly available in a dedicated register. These declarations will be removed from the register upon the dissolution of the AHWG, as outlined in Section 10. Similarly, if a member would withdraw or leave the AHWG prior to its dissolution, their declaration will be removed from the register at that time.

[9] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Available online at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049.

7. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725.[10] For further information, please refer to the data protection notice that is available as a separate document with the call.

8. REIMBURSEMENT OF MEMBERS

The members of this AHWG may be reimbursed for their expenses to participate in the meetings according to the ENISA internal rules for reimbursement. Members may be also subject to remuneration in case they undertake specific tasks, in line with ENISA's policy on remunerated external experts.

8.1 REIMBURSEMENT OF THE AHWG MEMBERS FOR THEIR TRAVEL AND SUBSISTENCE EXPENSES IN CONNECTION WITH THE ACTIVITIES OF THE AHWG

Members of an AHWG may be reimbursed for eligible travel and subsistence expenses incurred in relation to their participation within the AHWG. Reimbursement for the following expenses is available when travel is required from the member's official place of residence to another location:

1. **Travel expenses**: Economy-class airfare or first-class rail travel – whichever is more cost-effective – from the member's official place of residence to another European city.

2. **Daily Allowance**: A "daily subsistence allowance (DSA)" applicable to the country in which the meeting will take place. This allowance is set by the European Commission[11] and it covers all daily living expenses including hotel, meals, local travel etc.

3. **Other expenses**: No additional claims for living or travel costs will be accepted.

Members of the AHWG may choose to waive reimbursement on personal or professional grounds and will still remain eligible to participate. Representatives of Member States and observers in the AHWG are not remunerated or reimbursed, except in duly justified cases and subject to the approval of the AHWG Chair.

8.2 REIMBURSEMENT OF THE AHWG MEMBERS FOR ADDITIONAL TASKS

Remuneration: Members of the AHWG and of the AHWG reserve list that are citizens or permanent residents of the EU or EEA may be engaged in additional tasks conducted within or outside the scope of AHWG activities. In such case, the members of the AHWG shall be eligible for reimbursement under the same rules and procedures as those applicable for the ENISA CEI list of experts.[12]

[10] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. Available online at: https://eur-lex.europa.eu/eli/reg/2018/1725/oj.

[11] The latest rates are available to download from: https://international-partnerships.ec.europa.eu/document/download/16b30948-4166-4846-98bb-aa055be5fd75_en?filename=Per%20diem%20rates%20-%2025%20July%202022.pdf.

[12] CEI List of Individual External Experts to Assist ENISA | ENISA

The remuneration shall be based on the thresholds defined under Article 242 of the Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (Financial Regulation)[13] and under the following rules:

- **Daily fee**: The remuneration of the experts engaged from the list of the AHWG members shall be based on days of engagement and with a fixed daily fee of 450 euro.[14]
- **Maximum per annum**: The annual remuneration of a single expert shall in principle not exceed 30.000 euro.
- **Maximum remuneration**: The maximum amount of fees that can be paid to a single expert shall be 90 000 euro during a period of four consecutive calendar years.

AHWG members engaged by ENISA as remunerated experts may also be entitled to the reimbursement of expenses incurred in the course of journeys if invited to meetings organised by ENISA. In such case, the provisions of Article 8.1 shall apply.

Required documents: If the applicants for the AHWG wishes to be considered for additional remunerated tasks, they need to submit additional documents to their application, namely;

- **Legal and financial identification**: Proof of EU/EEA citizenship or permanent residence and proof of having a bank account in the EU member state or EEA.
- **Declaration on honour**: A declaration on their honour, in accordance with the template in Annex 1 to the present Call for expression of interest, duly signed and dated, stating that they are not in one of situations of exclusion as per criteria set out in the Article 138 of the Financial Regulation.

Validity: The validity period of the list of AHWG members - and reserve list – that may be considered for additional remunerated tasks shall follow the validity of the established AHWG.

8.3 TRANSPARENCY: EX-POST INFORMATION

If an expert is awarded a contract exceeding EUR 15,000, the expert's name, region of origin, contract amount, and subject matter shall be published on the contracting authority's website by 30 June of the year following the contract award. This information will remain publicly available for a period of two (2) years from the year of the contract award, after which it will be removed in accordance with applicable data retention and transparency policies.

[13] Regulation - EU, Euratom - 2024/2509 - EN - EUR-Lex.
[14] This is the maximum amount indicated in the Commission Decision establishing horizontal rules on the creation and operation of Commission expert groups C (2016) 3301 final.

9. APPLICATION PROCEDURE

9.1 CONDITIONS FOR MEMBERS

Individuals interested in joining the AHWG are invited to submit their application to ENISA by completing the application form available via the EU Survey tool, accessible through the dedicated section of the ENISA website.[15] Applicants who wish to be considered for additional tasks are encouraged to indicate their interest within the survey and upload the required supporting documents as specified in Section 8.2 of the Call for Expression of Interest.

Applications may be completed in any official language of the European Union. That being said, submission in English is strongly encouraged to facilitate the evaluation process. If another language is used, applicants are advised to include a summary of the CV and/or application in English.

The list of appointed members and permanent representatives will be made public in the ENISA website.

9.2 CONDITIONS FOR OBSERVERS

Public entities and organisations that represent a common interest and generally serve a public goal may apply to participate in the AHWG as permanent observers. These entities should submit an expression of interest clearly outlining:

- Their motivation for participating in the AHWG;
- The public interest or mandate they serve;
- The name and contact details of the proposed permanent observer.

The expression of interest must be addressed to the Executive Director of ENISA and sent to certification@enisa.europa.eu .Following review, the Executive Director may accept the participation of such organisations and their nominated representative as a permanent observer to the working group.

This application process is intended for public entities and stakeholder organisations other than those falling under the categories listed in section 4.2, which may designate their representatives to the AHWG directly to the Chairperson. These entities are expected to maintain an up-to-date list of their designated representatives to ensure continuity and accuracy over time.

9.3 DEADLINE FOR APPLICATIONS

Only applications submitted by the specified deadline will be considered admissible. The **deadline for submission is 20/07/2025, by 23.59 EET (Athens time).** The official date and time of submission will be determined by the timestamp generated by the European Commission's EU Survey tool, which is used to collect all applications.

This deadline does not apply to entities referred to in Section 4.2, which may participate as observers without a formal application. These entities shall inform the Chairperson of their designated representatives and promptly communicate any changes to ensure the accuracy of representation over time.

[15] https://ec.europa.eu/eusurvey/runner/Application-AHWG-EUMSS

10. TERMINATION OF THE MANDATE OF THE AD HOC WORKING GROUP AND DISSOLUTION

Once the tasks assigned to the AHWG have been completed, the group will enter its end-of-life phase and be formally disbanded. ENISA reserves the right to terminate the AHWG at any time should the need for its continued operation no longer exist.

Additionally, in the event of a shift in the priorities or structure of scheme – particularly where new service verticals would fall outside the scope of expertise identified under Section 11 – ENISA reserves the right to dissolve the AHWG and initiate a revised Call for Applications to address the new needs.

11. ELIGIBILITY CRITERIA

Only candidates who meet the minimum eligibility criteria based on their self-declared application forms will be considered for inclusion in the list of external experts, subject to endorsement by an evaluation committee. These mandatory criteria are as follows:

- The application form is fully completed;
- The applicant is either a national of or employed by a legal entity established in an EU Member State or EEA country;
- The applicant holds a bank account within the EU or EEA;
- Demonstrated proficiency in English as a working language;
- At least three years of relevant professional experience in the selected areas of expertise as per Section 12;
- A minimum of 12 months of relevant experience within the past five years;
- A motivation letter (maximum 500 words) explaining the applicant's interest in contributing to ENISA's work on EUMSS and demonstrating the ability to collaborate in a multicultural environment;
- A CV, preferably in Europass format.

The evaluation committee may, in exceptional cases, also consider applicants who are close to meeting the minimum experience thresholds or who possess a unique and relevant skillset that adds distinct value to the group's objectives.

12. SELECTION CRITERIA

To ensure a well-rounded group of experts supporting the development of EUMSS, ENISA will assess applications using the following criteria regarding horizontal and vertical competency domains.

Horizontal Competences	
Applicants should demonstrate horizontal experience across the MSS delivery lifecycle, including secure service and platform design, deployment and transition management a client organisations, availability and service continuity management, operational service management as well as continuous improvement and technology maintenance ensuring that MSS technologies remain secure and fit for purpose.	
MSS Design & Delivery	Applicants should demonstrate experience in the design or delivery of MSS solutions that embed security by default, translating recognised security frameworks into their client-facing solutions. They should demonstrate the ability to manage the secure deployment and transition processes, ensuring integration into client environments and maintaining service integrity.
MSS Availability & Continuity	Applicants should have experience in ensuring high availability and continuity of their MSS solutions, including familiarity with client recovery objectives, resilience planning, and incident response coordination. A strong understanding of operational service management is beneficial, particularly in maintaining service quality, managing SLAs, and integrating MSS within operational environments.
MSS Service Management	Applicants should demonstrate familiarity with practices that support continuous service improvement, such as vulnerability management, patching, lifecycle planning, and iterative risk mitigation.
Vertical Competences	
In addition to these horizontal competences, applicants are encouraged to demonstrate proven expertise in at least one vertical MSS domain:	
Incident Management	Applicants focusing on incident management should demonstrate experience in managing complex, large-scale cybersecurity incidents across diverse operational environments. Priority will be given to candidates who can show evidence of sustained, long-term involvement in incident response, coordination, and recovery – rather than individual projects. Candidates must be able to understand the complete incident lifecycle, from early detection and containment to remediation, reporting, and lessons learned, with a track record of continuous support in these domains.
Penetration Testing	Applicants with penetration testing expertise – whether in red, blue, or purple team capacities – should demonstrate practical experience conducting testing activities in complex client environments, including networks, cloud, virtualisation, ICS, and IoT systems. Evidence of end-to-end engagements is beneficial, including vulnerability reporting and remediation follow-up. Candidates should also possess a solid understanding of the technologies commonly used in penetration testing, along with established tools, methodologies, including novel and automated ones such as ones based on

	artificial intelligence, and frameworks that guide ethical hacking and security assessments.
Managed Security Operation Centres (SOC)	Applicants with experience in Security Operations Centre (SOC) are encouraged to apply, regardless of their operational delivery model, which can include fully managed SOC services or SOC support embedded within client environments. Experience on using artificial intelligence and data analytics in the context of SOCs as envisaged inter alia in the Cyber Solidarity Act is highly desirable. Experience in operating within multi-tenant or federated environments is particularly valued, given the complexity and scalability of MSS. Candidates should be able to demonstrate familiarity with common SOC technologies, tools and frameworks.
Cross-cutting Competences	
Applicants should demonstrate a strong understanding of the legal and regulatory landscape relevant to MSS, both at the EU and national levels. This includes familiarity with requirements imposed by the NIS 2 Directive, the Cyber Solidarity Act and the DORA Regulation. Candidates should also have practical experience in supporting or aligning with certification processes as well as the ability to interpret legal requirements and translate them into operational and technical controls.	

13. SELECTION PROCEDURE

The selection procedure will consist of an assessment of applications by ENISA, based on the selection criteria outlined in this Call. This assessment will be followed by the compilation of a shortlist of the most suitable candidates, concluding in the appointment of the ad hoc working group members by the Executive Director of ENISA.

ENISA promotes equal opportunities and accepts applications without any concern on grounds of sex, racial or ethnic origin, religion or belief, age or sexual orientation, marital status or family situation. The composition of the AHWG will strive for gender balance depending on applications likely to be received. Applications from disabled candidates are encouraged.

ANNEX 1

DECLARATION OF HONOUR ON EXCLUSION CRITERIA (FOR THE CANDIDATES WISHING TO BE FOR ADDITIONAL TASKS AS REMUNERATED EXPERTS)

Name:

"I hereby solemnly declare that I am not in one of the following situations:

I – SITUATION OF EXCLUSION CONCERNING THE PERSON

(1) **declares that** the above-mentioned person is in one of the following situations:	Y	N
(a) it is bankrupt, subject to insolvency or winding-up procedures, its assets are being administered by a liquidator or by a court, it is in an arrangement with creditors, its business activities are suspended or it is in any analogous situation arising from a similar procedure provided for under EU or national laws or regulations;	☐	☐
(b) it has been established by a final judgement or a final administrative decision that the person is in breach of its obligations relating to the payment of taxes or social security contributions in accordance with the applicable law;	☐	☐
(c) it has been established by a final judgement or a final administrative decision that the person is guilty of grave professional misconduct by having violated applicable laws or regulations or ethical standards of the profession to which the person belongs, or by having engaged in any wrongful conduct which has an impact on its professional credibity where such conduct denotes wrongful intent or gross negligence, including, in particular, any of the following:		
(i) fraudulently or negligently misrepresenting information required for the verification of the absence of grounds for exclusion or the fulfilment of selection criteria or in the performance of a contract or an agreement;	☐	☐
(ii) entering into agreement with other persons with the aim of distorting competition;	☐	☐
(iii) violating intellectual property rights;	☐	☐
(iv) unduly influencing or attempting to unduly influence the decision-making process to obtain Union funds by taking advantage, through misrepresentation, of a conflict of interests involving any financial actors or other persons referred to in Article 61(1) FR;	☐	☐

(v) attempting to obtain confidential information that may confer upon it undue advantages in the award procedure*;*	☐	☐
(vi) incitement to discrimination, hatred or violence against a group of persons or a member of a group or similar activities that are contrary to the values on which the Union is founded enshrined in Article 2 TEU, where such misconduct has an impact on the person's integrity which negatively affects or concretely risks affecting the performance of a contract or an agreement;	☐	☐
(d) it has been established by a final judgement that the person is guilty of the following:		
(i) fraud, within the meaning of Article 3 of Directive (EU) 2017/1371 and Article 1 of the Convention on the protection of the European Communities' financial interests, drawn up by the Council Act of 26 July 1995;	☐	☐
(ii) corruption, as defined in Article 4(2) of Directive (EU) 2017/1371 and Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, drawn up by the Council Act of 26 May 1997, and conduct referred to in Article 2(1) of Council Framework Decision 2003/568/JHA, as well as corruption as defined in the applicable law;	☐	☐
(iii) conduct related to a criminal organisation, as referred to in Article 2 of Council Framework Decision 2008/841/JHA;	☐	☐
(iv) money laundering or terrorist financing, within the meaning of Article 1(3), (4) and (5) of Directive (EU) 2015/849 of the European Parliament and of the Council;	☐	☐
(v) terrorist-related offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Council Framework Decision 2002/475/JHA, respectively, or inciting, aiding, abetting or attempting to commit such offences, as referred to in Article 4 of that Decision;	☐	☐
(vi) child labour or other offences concerning trafficking in human beings as referred to in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council;	☐	☐
(e) it has shown significant deficiencies in complying with the main obligations in the performance of a contract or an agreement financed by the Union's budget, which has led to its early termination or to the application of liquidated damages or other contractual penalties, or which has been discovered following checks, audits or investigations by a contracting authority, the European Anti-Fraud Office (OLAF), the Court of Auditors or the European Public Prosecutor's Office (EPPO);	☐	☐

(f) it has been established by a final judgment or final administrative decision that the person has committed an irregularity within the meaning of Article 1(2) of Council Regulation (EC, Euratom) No 2988/95;	☐	☐
(g) it has been established by a final judgment or final administrative decision that the person has created an entity under a different jurisdiction with the intent to circumvent fiscal, social or any other legal obligations in the jurisdiction of its registered office, central administration or principal place of business.	☐	☐
(h) (*only for legal persons*) it has been established by a final judgment or final administrative decision that the person has been created with the intent provided for in point (g).	☐	☐
(i) for the situations referred to in points (c) to (h) above the person is subject to: i. facts established in the context of audits or investigations carried out by the European Public Prosecutor's Office after its establishment, the Court of Auditors, the European Anti-Fraud Office (OLAF) or the internal auditor, or any other check, audit or control performed under the responsibility of an authorising officer of an EU institution, of a European office or of an EU agency or body; ii. non-final administrative decisions which may include disciplinary measures taken by the competent supervisory body responsible for the verification of the application of standards of professional ethics; iii. facts referred to in decisions of entities or persons being entrusted with EU budget implementation tasks; iv. information transmitted by Member States implementing Union funds; v. decisions of the Commission relating to the infringement of Union competition law or of a national competent authority relating to the infringement of Union or national competition law; or vi. informed, by any means, that it is subject to an investigation by the European Anti-Fraud office (OLAF): either because it has been given the opportunity to comment on facts concerning it by OLAF, or it has been subject to on-the-spot checks by OLAF in the course of an investigation, or it has been notified of the opening, the closure or of any circumstance related to an investigation of the OLAF concerning it.	☐	☐

Name and Surname:

Date: **Signature:**