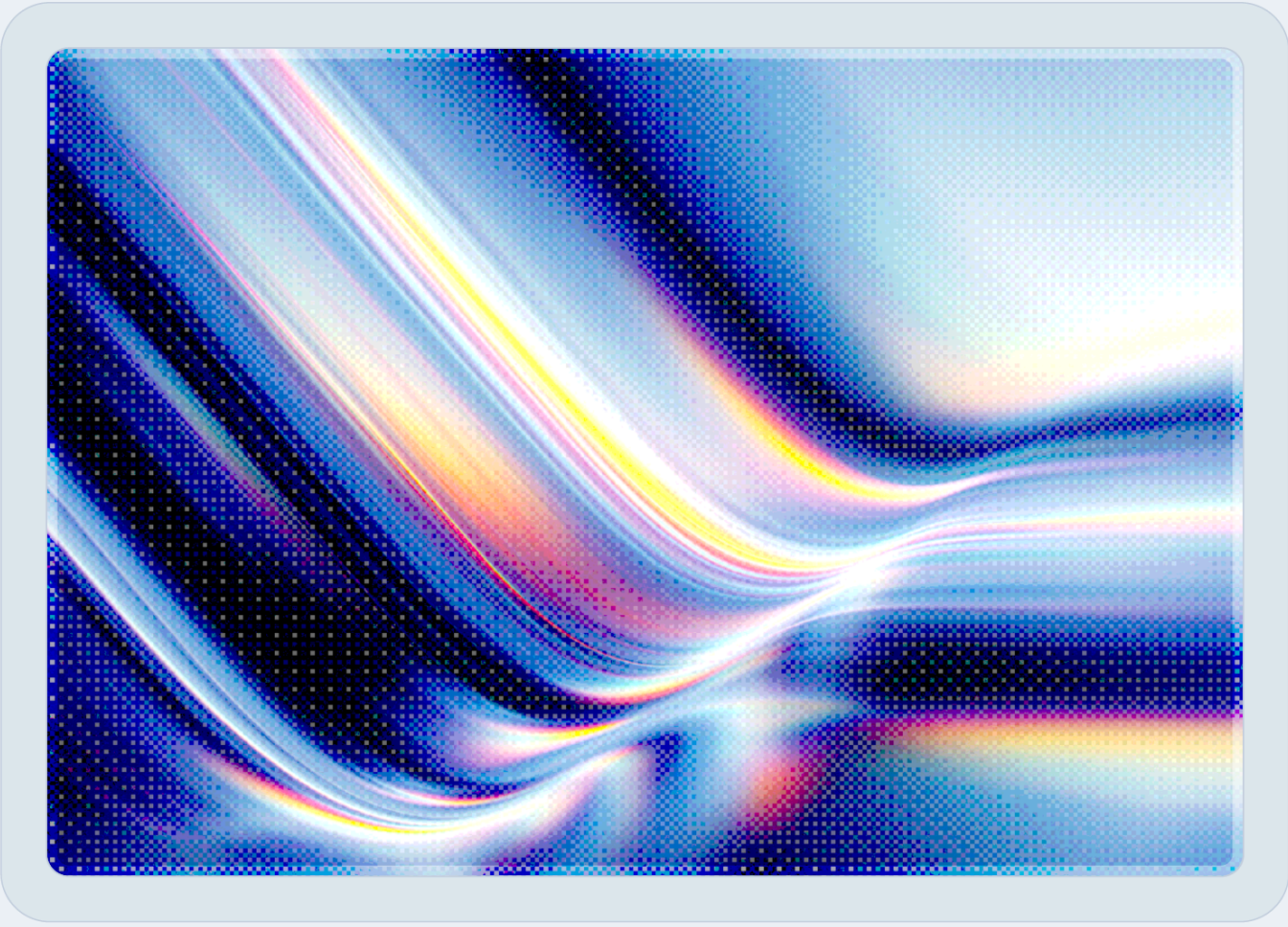
CSAI Foundation | Cloud Security Alliance

ENISA's Draft EU Certification Scheme for Managed Security Services

2026-08-27

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

ENISA opened a public consultation on July 24, 2026, on the draft candidate European cybersecurity certification scheme for Managed Security Services, known as EUMSS, with stakeholder comments due by September 13, 2026 [2]. The scheme responds to a formal request the European Commission made to ENISA in April 2025, under the authority created when the Cybersecurity Act was amended in early 2025 to bring managed security services within its certification framework for the first time [3][4]. As drafted, EUMSS organizes requirements into a horizontal layer of baseline controls that would apply to every certified managed security service, spanning secure design, deployment management, availability and continuity, operational management, and continuous improvement, plus vertical layers of service-specific requirements that today cover only incident response, with detection and recovery profiles expected later [3][5]. The draft sets three assurance levels, basic, substantial, and high, mirroring the tiered model already used elsewhere in EU cybersecurity certification [3]. Certification under EUMSS will also become a gating requirement for providers seeking to deliver services through the EU Cybersecurity Reserve, which must certify within two years of the scheme becoming operational [1][6]. For CISOs and MSSPs operating in or selling into the EU, the consultation window is a limited opportunity to shape requirements before the scheme is finalized and certification becomes a practical gating condition for Reserve eligibility and, likely, vendor risk expectations under NIS2.

Background

Managed security services, incident response, penetration testing, security monitoring, security audits, and cybersecurity advisory work, have become a significant channel through which organizations obtain cybersecurity capability, reflecting a broader industry trend toward outsourcing specialized security functions [4][7]. ENISA has observed that this shift toward outsourcing has occurred without a corresponding harmonization of the requirements that apply to the providers delivering these services, producing a patchwork of national rules, informal accreditation practices, and inconsistent quality assurance across EU Member States [4]. This fragmentation plausibly creates friction for MSSPs operating cross-border and may leave customers with a limited basis for comparing providers on security assurance, though ENISA's own materials frame the harmonization goal primarily in market and quality terms [4].

The European Cybersecurity Act, which already underpins EU-wide certification schemes for ICT products, services, and processes such as EUCC for products and EUCS for cloud services, did not originally extend to managed security services. That changed when the Commission adopted Regulation (EU) 2025/37, which entered into force in February 2025 and amended the Cybersecurity Act specifically to enable a certification scheme covering MSS [1][6]. The Commission formally requested that ENISA prepare a candidate scheme on April 25, 2025, invoking its mandate under Article 48(1) of the Cybersecurity Act [1][4]. ENISA subsequently opened a call for experts on June 25, 2025, and convened an Ad Hoc Working Group with Member State representatives and technical experts that held its kickoff meeting on October 13, 2025 [3]. That working group produced the draft scheme now open for public review.

The initiative is also linked to the EU Cybersecurity Solidarity Act and its EU Cybersecurity Reserve, a pool of vetted incident response providers that Member States and EU institutions can call on during large-scale cybersecurity incidents. ENISA Executive Director Juhan Lepassaar has framed the certification effort as essential "to ensure a certain level of quality and security of services offered in the Single Market," and noted that the scheme will help "facilitate the selection of trusted providers for the EU Cybersecurity Reserve" [1]. Once EUMSS becomes operational, providers wishing to deliver services under the Reserve umbrella will have two years to obtain certification [1][6].

Security Analysis

The draft scheme's two-layer architecture is its central design choice, and it has direct implications for how MSSPs will need to structure their compliance programs. The horizontal layer functions as a baseline that every certified provider must satisfy regardless of which specific service they deliver, covering secure design of service delivery infrastructure, controls over how services are deployed and managed for customers, requirements for availability and continuity of the service itself, day-to-day operational management practices, and processes for continuous improvement of the service over time [3]. Layered on top, vertical requirements address the technical specifics of a given service category; the draft currently defines a profile only for incident response, with ENISA signaling that detection and recovery profiles will follow in later iterations [3][6]. This mirrors the layered approach already used in EUCS for cloud services, and it means providers offering multiple types of managed security services, for example both incident response and penetration testing, may eventually need to certify separately against each vertical profile while satisfying a shared set of horizontal controls once.

The table below summarizes the draft scheme's current structure as reflected in ENISA's published materials. It is a point-in-time snapshot; the working group is expected to expand vertical coverage in subsequent drafts.

Layer	Element	Current Scope
Horizontal (baseline)	Secure design	Applies to all certified MSS regardless of type [3]
Horizontal (baseline)	Deployment management	Applies to all certified MSS regardless of type [3]
Horizontal (baseline)	Availability and continuity	Applies to all certified MSS regardless of type [3]
Horizontal (baseline)	Operational management	Applies to all certified MSS regardless of type [3]
Horizontal (baseline)	Continuous improvement	Applies to all certified MSS regardless of type [3]
Vertical (service-specific)	Incident response	Only profile defined in the current draft [3][6]
Vertical (service-specific)	Detection, recovery	Planned for future iterations, not yet published [3][6]
Vertical (service-specific)	Penetration testing, security audits, consultancy	Named in scheme's target scope but no profile drafted yet [3][6]
Assurance levels	Basic, substantial, high	Three tiers, consistent with EUCC and EUCS conventions [3]

Because only the incident response profile currently exists, organizations that rely on MSSPs for penetration testing, security audits, or advisory services should not expect near-term certification coverage for those service categories even after EUMSS formally launches. This gap between the scheme's stated long-term scope and its initial vertical coverage is itself worth flagging in consultation comments, since stakeholders with a stake in faster coverage of other service types have a direct interest in signaling that priority to the working group now, before the scheme's initial version is finalized.

The three-tier assurance model, basic, substantial, and high, follows the structure already established under EUCC and EUCS, giving providers and customers a familiar reference point for comparing assurance rigor across schemes [3]. However, because the vertical layer is still limited to incident response, the practical scope of what can be certified at launch will be narrower than the full definition of

managed security services the scheme ultimately intends to cover, which spans incident response, penetration testing, security audits, and consultancy [3][6]. Organizations relying on MSSPs for services outside the initial incident response profile will need to track subsequent working group output rather than assume immediate coverage.

The tie to the EU Cybersecurity Reserve raises the practical stakes for Reserve-eligible providers considerably. Because Reserve-eligible providers face a hard two-year certification deadline once the scheme is finalized, MSSPs that want to remain eligible for Reserve engagements have a direct commercial incentive to review the draft now and flag any requirements that would be difficult to meet operationally [1][6]. More broadly, because EUMSS will interact with obligations under the NIS2 Directive, which already requires many essential and important entities to manage supply chain and third-party security risk, a finalized EUMSS certification could become a de facto reference point that NIS2-regulated entities look to when selecting or auditing their managed security providers, even though EUMSS itself is a voluntary certification scheme rather than a NIS2 mandate.

A further consideration is how EUMSS will sit alongside existing national accreditation regimes and sector-specific requirements that some Member States already impose on providers of incident response or security monitoring services. ENISA has framed the fragmentation of these national approaches as the core problem EUMSS is meant to solve, but a voluntary EU-wide scheme does not automatically supersede national requirements, and providers operating across multiple Member States may need to maintain both national accreditations and EUMSS certification during a transition period [4]. The working group's choice to build EUMSS on the same layered, tiered-assurance model already used in EUCC and EUCS would, if intentional, ease this coexistence: providers and conformity assessment bodies already familiar with those schemes should face a lower learning curve when EUMSS enters force. ENISA has not stated this rationale explicitly, but the practical burden of dual compliance during any transition window remains a real cost that stakeholders should raise during the consultation [3].

The consultation also arrives at a moment when AI-assisted tooling is increasingly used in detection, triage, and incident-response workflows industry-wide, from AI-augmented security monitoring platforms to generative-AI-assisted report drafting during incident response engagements. The current draft's horizontal domains, particularly secure design and continuous improvement, appear broad enough to potentially encompass the tooling and processes a provider uses to deliver a service, not only the service's output [3], though the draft does not address AI tooling explicitly. Providers that have adopted AI-assisted delivery models may want to consider whether their current AI governance practices would satisfy an assessor evaluating those domains once the scheme is operational. This is an area where the current draft offers limited specificity, and it represents another concrete point stakeholders can raise during the consultation window.

Recommendations

Immediate Actions

Organizations that provide or consume managed security services in the EU should review the draft EUMSS scheme documentation available through ENISA's certification portal and assess whether the proposed horizontal baseline and incident response vertical profile align with their current operating model [3][5]. MSSPs, industry associations, and conformity assessment bodies with a stake in the outcome should submit comments through the EU Survey tool before the September 13, 2026 deadline, since the consultation is explicitly open to public authorities, providers, industry representatives, conformity assessment bodies, and academia [1][2].

Short-Term Mitigations

CISOs who procure incident response, penetration testing, or security monitoring services should begin mapping their current MSSP contracts against the horizontal domains described in the draft, secure design, deployment management, availability and continuity, operational management, and continuous improvement, to identify gaps before certification requirements become binding [3]. Procurement and legal teams negotiating new MSSP agreements should consider including provisions anticipating eventual EUMSS certification, particularly for providers that may seek EU Cybersecurity Reserve eligibility.

Strategic Considerations

Enterprises with EU operations subject to NIS2 supply chain risk management obligations should plan to incorporate EUMSS certification status into vendor risk assessment criteria once the scheme is adopted, even though certification will initially remain voluntary outside the Reserve context. MSSPs should also monitor the pace at which ENISA extends vertical profiles beyond incident response, since the scheme's practical value to customers would likely grow as coverage expands to penetration testing, security audits, and advisory services.

CSA Resource Alignment

CSA's prior work on European certification harmonization provides direct grounding for evaluating EUMSS. "The European Cloud Certification Scheme: Forward Together," developed through CSA's CSPCERT Working Group, documents industry recommendations for implementing a harmonized EU cloud security certification scheme under the Cybersecurity Act, and its analysis of how a layered, Member-State-coordinated certification process should function applies directly to assessing EUMSS's own horizontal and vertical layer design [8]. CSA's briefing "How Cybersecurity Certification can Foster the EU Cybersecurity Market" similarly examines how EU-wide certification frameworks affect provider competitiveness and market trust, offering relevant context for MSSPs weighing the commercial implications of pursuing EUMSS certification once it becomes tied to EU Cybersecurity Reserve eligibility [9]. Organizations evaluating governance and control mappings for their own managed security service delivery, whether they are pursuing EUMSS certification or assessing an MSSP's readiness for it, can also use CSA's AI Controls Matrix (AICM) v1.1 as a broader assurance and control reference, particularly as AI-assisted tooling becomes more common in incident response and security monitoring service delivery [10].

References

[1] ENISA. "EU Managed Security Services Certification to drive the cybersecurity market." ENISA, June 2025.

[2] ENISA. "Have your say on the certification of EU Managed Security Services." ENISA, July 24, 2026.

[3] ENISA. "Draft Candidate EUMSS Scheme v1.1 – Public Review." European Union Cybersecurity Certification, 2026.

[4] NCCA (Cyprus National Cybersecurity Certification Authority). "ENISA Launches Public Consultation on the Draft EU Certification Scheme for Managed Security Services." NCCA, 2026.

[5] European Commission. "EU Survey: Public Review EUMSS." EUSurvey, 2026.

[6] Global Security Mag. "Have your say on the certification of EU Managed Security Services." Global Security Mag, 2026.

[7] Industrial Cyber. "ENISA launches draft EUMSS cybersecurity certification scheme for managed security services, seeks feedback." Industrial Cyber, 2026.

[8] Cloud Security Alliance. "The European Cloud Certification Scheme: Forward Together." Cloud Security Alliance, 2025.

[9] Cloud Security Alliance. "How Cybersecurity Certification can Foster the EU Cybersecurity Market." Cloud Security Alliance, 2025.

[10] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2025.

