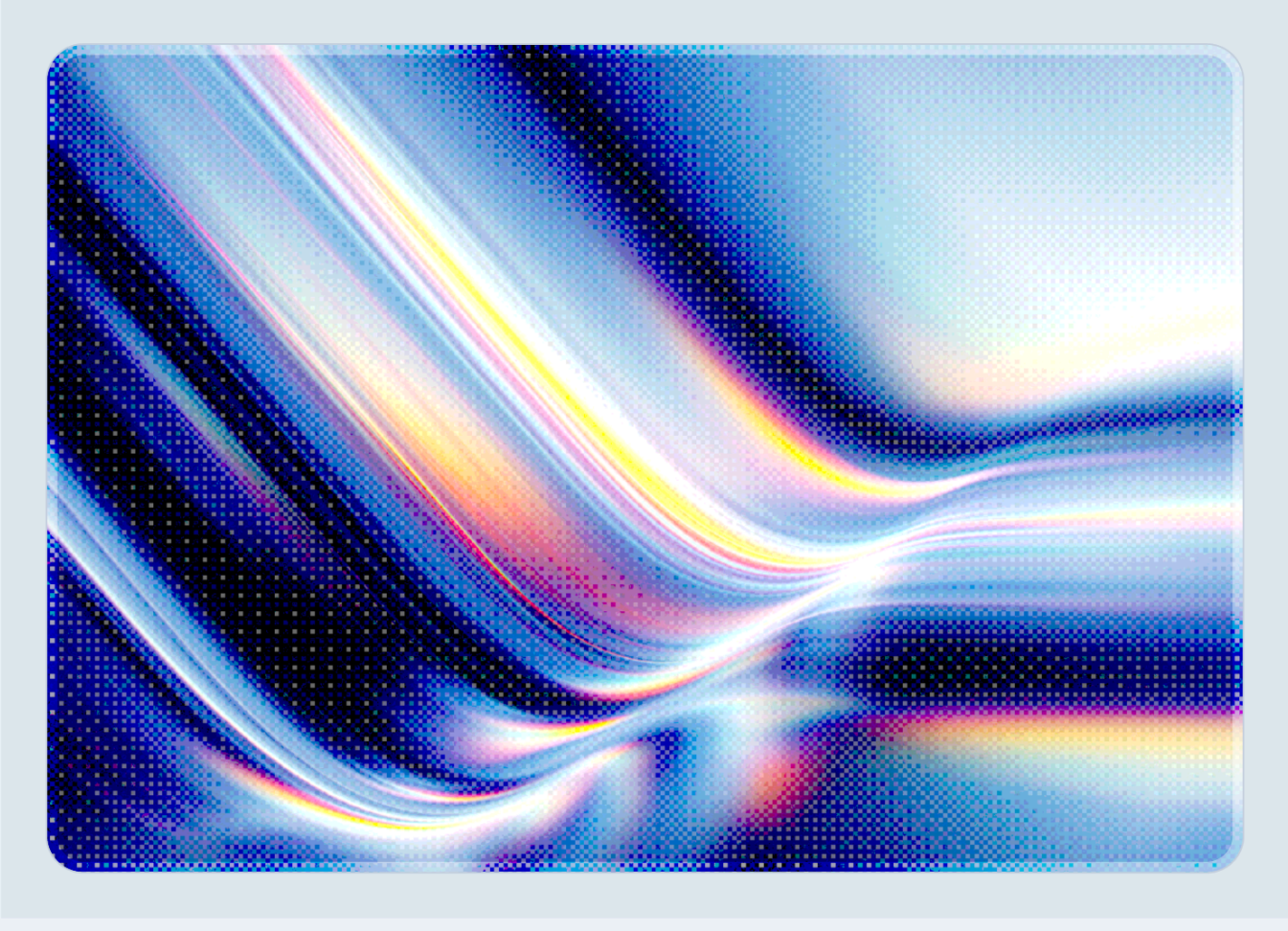
CSAI Foundation | Cloud Security Alliance

ENISA NCAF 2.0: EU Cybersecurity Maturity Framework Aligned to NIS2

2026-04-27

Unofficial AI-assisted Research



CSAI

CSA cloud security alliance®

Key Takeaways

ENISA published the National Capabilities Assessment Framework 2.0 (NCAF 2.0) on April 22, 2026, replacing the original 2020 framework with a methodology rebuilt to support EU Member States preparing for the voluntary peer review process introduced under Article 19 of the NIS2 Directive [1][2][3]. The update widens the assessment scope from the original seventeen objectives to twenty strategic objectives organised into four thematic clusters — capacity building and awareness, cooperation and collaboration, cybersecurity governance, and regulatory and policy frameworks — and reorganises the maturity scoring so that results aggregate cleanly at the objective, cluster, and overall national levels [3][4]. According to trade reporting on lessons learned from the framework's pilot in Greece, Italy, and Luxembourg, Member States that complete the assessment can expect to invest roughly fifteen person-days of cross-government coordination per assessment cycle, per Member State [4].

The framework's policy weight comes from where it sits in the EU cybersecurity stack rather than from any new technical control. Article 19 of NIS2 obliges the NIS Cooperation Group to run peer reviews, with ENISA and the Commission acting as observers, and gives reviewing experts the right to examine risk-management measures, competent authority capabilities, CSIRT operational capacity, mutual assistance, information sharing, and cross-border or sector-specific issues [5][6]. NCAF 2.0 is the self-assessment instrument ENISA expects national authorities to use to prepare those reviews, and trade reporting on the framework indicates that it now incorporates requirements drawn from NIS2 Articles 7, 19, 21, and 23 alongside the broader EU Cybersecurity Index reporting cycle [4]. For organisations operating under NIS2 — and for cloud and AI service providers whose customers are essential or important entities — the framework signals which national capabilities will be measured, which gaps Member States are most likely to close first, and which sectoral demands are positioned to flow downstream into procurement and supply-chain rules.

Three findings matter most for security teams. First, NCAF 2.0 is voluntary at the Member State level but its outputs feed the Article 19 peer review record and the EU Cybersecurity Index, so the framework's signals are likely to reach procurement officers and regulators even where formal mandates do not [2][7]. Second, supply chain cybersecurity, vulnerability handling, and AI-related ICT supply chain considerations sit explicitly inside the regulatory and policy frameworks cluster, meaning Member States will be asked to demonstrate that policy levers exist for those domains regardless of whether national legislation has yet caught up [3][8]. Third, AI-specific maturity is not assessed in NCAF 2.0 itself but is pulled into the same orbit through ENISA's Multilayer Framework for Good Cybersecurity Practices for

AI (the agency's FAICP work) and the EU AI Act, with the practical consequence that cloud providers and AI vendors selling into Europe should expect their national customers to be benchmarked on AI-supply-chain readiness even though that work is not yet visible in NCAF scoring [9][10].

Background

What NCAF Is and Why It Was Updated

ENISA published the original National Capabilities Assessment Framework in December 2020 with the help of subject-matter experts and representatives from nineteen Member States and EFTA countries [11]. That first version organised seventeen strategic objectives derived from common priorities across published National Cybersecurity Strategies (NCSS) into four clusters and five maturity levels, and it was designed primarily as a self-assessment tool to help governments improve their NCSS lifecycle. Five years later, the policy environment around it has changed substantially. The NIS2 Directive entered into force in January 2023 and required transposition by October 2024, the Cyber Resilience Act and DORA introduced supply-chain and operational-resilience obligations, and ENISA itself published the EU Cybersecurity Index alongside the NIS360 sectoral maturity assessment [7][12].

The 2.0 update closes the gap between the assessment instrument and that policy environment. ENISA describes NCAF 2.0 as a methodology for national authorities to "strengthen their cybersecurity capabilities and assess the maturity of national cybersecurity strategies' implementation," with explicit hooks into the new NIS2 obligations [1]. The number of strategic objectives has grown from seventeen to twenty to capture areas — vulnerability disclosure coordination, supply chain instruments, and incident reporting under NIS2 — that the original framework treated less directly [3][4]. Maturity descriptors have been rewritten to reflect today's threat landscape, and the cluster boundaries have been redrawn so that an assessment can produce a coherent picture for the peer review process under Article 19 [1][3].

The NIS2 Article 19 Peer Review Anchor

Article 19 of NIS2 establishes a voluntary peer review mechanism intended to "achieve a high common level of cybersecurity" and to enhance "Member States' cybersecurity capabilities and policies necessary to implement the Directive" [5]. The Cooperation Group, supported by the Commission and ENISA, was required to establish the methodology and organisational aspects of these reviews by January 17, 2025; ENISA's publication of NCAF 2.0 in April 2026 is the operational instrument that supports that methodology in practice. Reviews are carried out by experts designated by at least two Member States other than the one being reviewed, and they may include both physical and virtual on-site visits as well as

off-site information exchanges [5][6]. The scope is open to any of six areas listed in the Directive: risk-management measures, the capabilities of competent authorities, the operational capacity of CSIRTs, the implementation of mutual assistance, information-sharing arrangements, and cross-border or sector-specific issues [5].

NCAF 2.0 matters in this context because peer reviews are most useful when they have a comparable evidence base across Member States, and the Article 19 methodology does not itself prescribe an internal-evidence template. ENISA positions NCAF 2.0 as that template: the framework structures the self-assessment that a reviewed Member State can hand to designated experts, supports the gap-identification work that those experts then probe, and produces scoring that can be reused for the EU Cybersecurity Index and for ENISA's annual State of Cybersecurity in the Union report [1][2][7]. ENISA and the Commission participate in peer reviews as observers and provide secretariat support, which means insights from NCAF self-assessments can inform the broader EU posture without the framework itself becoming a binding rule [5].

How the Framework Is Structured

The framework's twenty strategic objectives are grouped into four clusters that map to the operational priorities Member States articulate in their NCSS documents [3][4]. The capacity building and awareness cluster covers cyber resilience, cyber hygiene, the skills gap, research and development, incident preparedness, and public awareness. The cooperation and collaboration cluster covers stakeholder cooperation, information sharing, mutual assistance, international cooperation, and the response to cybercriminal activity. The cybersecurity governance cluster covers governance practices, risk management, crisis management, incident reporting, and trust in digital services. The regulatory and policy frameworks cluster covers supply chain instruments, active cyber protection, critical infrastructure protection, and the policy levers needed to safeguard ICT products and services. Together these twenty objectives generate the questions that drive the maturity scoring.

Each objective is assessed against five maturity levels that move from foundational, uncoordinated effort up through a developing posture, an established baseline, a mature performance-based regime, and an advanced adaptive capability that can absorb emerging threats [13]. Trade reporting on the pilot indicates that the underlying questionnaire contains roughly 870 tailored capacity questions plus five generic strategy maturity questions per objective per level, with scoring rolled up at the objective, cluster, and global levels so that progress can be tracked over time [4]. The accompanying online tool, also published on April 22, 2026, allows national authorities to capture answers, attach evidence, and produce a structured output that can be exchanged with peer-review experts [1][2].

The cluster-to-Article mapping below illustrates how each cluster is positioned against the obligations Member States are simultaneously trying to satisfy under NIS2. The article anchors for the regulatory, policy, governance, and cooperation rows include analyst-derived mappings beyond those explicitly named in the cited trade reporting; the official Article-to-cluster mapping is published in the ENISA NCAF 2.0 framework document.

Cluster	Focus	NIS2 Article Anchors
Capacity building and awareness	Cyber resilience, skills, R&D, incident preparedness, awareness	Articles 7, 18
Cooperation and collaboration	Stakeholder cooperation, information sharing, mutual assistance, cybercrime response	Articles 7, 13, 17, 19
Cybersecurity governance	Governance, risk management, crisis management, incident reporting	Articles 7, 9, 21, 23
Regulatory and policy frameworks	Supply chain, critical infrastructure, ICT product policy, vulnerability handling	Articles 7, 21, 22

Sources: ENISA NCAF 2.0 framework summary [3][4], NIS2 Directive [5][14]; cluster-row article anchors beyond Articles 7, 19, 21, and 23 are analyst-derived from the NIS2 article texts.

Security Analysis

What Changed Between NCAF 1.0 and 2.0

The most consequential structural change is the explicit alignment with NIS2 articles. NCAF 1.0 was published before NIS2 was adopted and was therefore organised around the older NIS Directive and ENISA's NCSS lifecycle work. Trade reporting on NCAF 2.0 indicates that the new methodology incorporates requirements drawn from Articles 7 (national cybersecurity strategy), 19 (peer reviews), 21 (cybersecurity risk-management measures), and 23 (incident reporting), which means the assessment now mirrors the obligations Member States are simultaneously trying to satisfy under the Directive [4][5]. The shift from seventeen to twenty objectives is the most visible expression of this alignment, with the additions concentrated in supply-chain policy, vulnerability disclosure coordination, and incident-handling readiness – areas where NIS2 introduces concrete national obligations.

Two other changes affect how the framework is used in practice. First, the maturity descriptions across all five levels were rewritten to reflect a more dynamic threat picture; ENISA describes the result as a continuum from "foundation" through "advanced" that emphasises adaptability and forward-looking capability rather than steady-state compliance [13]. Second, the questionnaire was expanded and rebalanced so that scoring at the objective and cluster level produces a usable benchmark for the EU Cybersecurity Index, with ENISA explicitly noting that it intends NCAF outputs and the EU-CSI to be complementary [4][7]. The pilot Member States — Greece, Italy, and Luxembourg — used the redesigned framework on production NCSS work. Pilot reports note improvements in gap identification, prioritisation, and policy-cycle planning, alongside a request from Luxembourg for further simplification of the questionnaire — a signal that the fifteen person-day cost remains a meaningful adoption barrier and that the pilot evidence base is small enough that improvement claims should be read as directional rather than definitive [4].

Implications for Cloud and AI Service Providers

NCAF 2.0 measures national capabilities, not provider behaviour, but the assessment will indirectly shape what providers are asked to demonstrate to their European customers. The regulatory and policy frameworks cluster scores Member States on whether they have policy instruments for supply chain cybersecurity, ICT product and service security, and active cyber protection [3][8]. Member States that score themselves as immature in those areas are likely to respond by tightening procurement language, introducing certification preferences, or accelerating transposition of related EU instruments such as the Cyber Resilience Act and the EU Cybersecurity Certification Schemes. Cloud, SaaS, and AI vendors should anticipate that European tender questionnaires may begin to mirror the NCAF objectives more closely — particularly in the areas of incident reporting, supply-chain risk management, and crisis management — because national authorities have a structural incentive to push their own observed gaps onto the providers that serve essential and important entities.

The AI dimension is not assessed directly inside NCAF 2.0, but it sits adjacent to the framework in two important ways. First, ENISA's Multilayer Framework for Good Cybersecurity Practices for AI (referred to publicly as FAICP) is positioned as the agency's response to the EU AI Act and treats the AI supply chain as a domain that requires its own cybersecurity controls [9][10]. Second, the EU Cybersecurity Index and the State of Cybersecurity in the Union report consider AI-driven threats and AI-enabled defenses when describing national posture [7]. The practical effect for AI providers is that even though "AI" does not appear as a separate maturity objective in NCAF 2.0, the supply-chain, governance, and incident-handling objectives in the framework will be applied by national reviewers to AI systems where those systems are integrated into essential services. Providers who can demonstrate readiness against CSA's AI Controls Matrix (AICM) and the MAESTRO threat-modelling framework will find it easier to evidence that readiness in the procurement and audit cycles that follow Member State self-assessments.

Where the Framework Stops

Three limitations are worth flagging for security leaders relying on NCAF 2.0 as a planning anchor. The framework is voluntary at the Member State level and Article 19 peer reviews are likewise voluntary, so there is no single deadline by which all twenty-seven Member States will have produced comparable scores [2][5]. The methodology is a self-assessment with peer-review validation rather than an external audit, which means the comparability of scores across Member States depends on consistent interpretation of the maturity descriptors and on the willingness of governments to be candid about gaps. And the framework focuses on national-level capabilities rather than entity-level controls, so it cannot substitute for the operational risk-management measures that essential and important entities must implement under Article 21 of NIS2.

These limitations are by design. NCAF 2.0 is intended to drive policy and investment prioritisation at the Member State level, with the EU Cybersecurity Index providing comparative posture data and the NIS360 product providing sectoral maturity insight [7][12]. Security teams that treat NCAF as a strategic planning input rather than a compliance instrument will get more value from it. This research note is a point-in-time analysis as of April 27, 2026; it does not predict specific Member State adoption timelines and the inferences about provider procurement effects should be read as analyst projections rather than observed outcomes.

Recommendations

Immediate Actions (Next 30 Days)

EU-headquartered organisations and providers serving European essential or important entities should begin by reading the NCAF 2.0 publication and the accompanying online tool, mapping their existing control evidence to the four clusters, and identifying which of the twenty objectives are most likely to surface in their national authority's self-assessment [1][3]. Where an organisation is part of the supply chain for an essential entity, it is reasonable to anticipate that the customer will pass NCAF-derived questions through to vendors during contract renewal cycles, so security teams should pre-build evidence packs against the supply chain, incident reporting, and risk-management objectives before those requests arrive.

Information security and compliance teams should also confirm that the organisation's incident notification posture aligns with the cascading deadlines defined in Article 23 of NIS2, since incident reporting maturity is one of the most directly observable elements of the cybersecurity governance cluster and one that national authorities will themselves be measured against [14]. Boards and risk

committees of multi-national organisations should be briefed that NCAF 2.0 has been published and that it is positioned to shape both the EU peer-review cadence and the questions that European customers ask.

Short-Term Mitigations (Next 90 Days)

Over the next quarter, organisations should align internal control evidence with the NCAF cluster structure rather than with any single national questionnaire. This means producing a control inventory that maps to capacity building and awareness, cooperation and collaboration, cybersecurity governance, and regulatory and policy frameworks — using CSA's AI Controls Matrix and the Cloud Controls Matrix as the underlying control set — so that the same evidence can be reused across multiple national jurisdictions. Cloud providers should review their published shared-responsibility documentation to ensure that supply-chain provenance, vulnerability handling, and incident-reporting commitments are explicit and verifiable, because those are the objectives in NCAF 2.0 most likely to be probed.

For organisations developing or hosting AI systems used by EU essential or important entities, the same ninety-day window should be used to align FAICP-style AI cybersecurity evidence with the NCAF supply-chain and governance objectives. ENISA's FAICP work treats the AI supply chain as a first-class concern, and AICM provides a control set that maps to it; the gap most likely to appear in customer audits is between an organisation's AI risk-management posture and the supply-chain-specific evidence required by NCAF reviewers [9][10].

Strategic Considerations (12 Months and Beyond)

Strategically, NCAF 2.0 should be read as confirmation that Europe is converging on a measured, comparative approach to national cybersecurity that uses ENISA-produced indices to drive both peer review and EU-level reporting. Organisations should expect that the EU Cybersecurity Index, NCAF 2.0, NIS360, and the State of Cybersecurity in the Union report will progressively interlock, with the result that capabilities benchmarked at the national level will increasingly inform sector-specific obligations. CSA-aligned organisations can anticipate this trajectory by participating in CSA's European working groups on AI controls, cloud governance, and AICM implementation, and by contributing implementation evidence that helps Member States populate the new objectives credibly.

A second strategic consideration is the long-term relationship between NCAF and the EU AI Act. As FAICP matures and the AI Act's high-risk system obligations take effect through 2026, ENISA may extend NCAF 2.0 with AI-specific objectives or publish a complementary instrument that focuses on AI capabilities at the Member State level. Organisations would be well advised to treat their AI supply-chain

controls as a domain likely to be assessed within the medium term, even if it is not directly assessed today, and to invest in the documentation, attestation, and provenance practices that an ENISA-style maturity framework would require.

CSA Resource Alignment

The objectives within NCAF 2.0 align with several existing CSA frameworks that European organisations can use to operationalise national-level expectations into entity-level controls. The AI Controls Matrix (AICM) provides the AI-specific control set that should sit alongside FAICP for any organisation building or operating AI systems for European customers; AICM is a superset of the Cloud Controls Matrix (CCM) and therefore covers the cloud foundations on which many regulated AI systems are deployed. The MAESTRO framework for agentic AI threat modelling supports the risk-management and incident-preparedness objectives in NCAF's governance cluster by providing structured threat enumeration that can be referenced in national risk assessments. CSA's Zero Trust Guidance and the AI Organizational Responsibilities work give boards and CISOs the governance language they need to translate NCAF cluster results into accountable internal mandates.

CSA's STAR (Security, Trust, Assurance and Risk) registry is the most direct supply-chain attestation instrument available to providers serving European essential and important entities. STAR-attested cloud and AI providers can offer national authorities and their customers a third-party-validated evidence trail that aligns with several of the supply-chain and governance objectives in NCAF 2.0, supporting Member States that need to evidence supply-chain maturity in peer reviews. Together, AICM, MAESTRO, STAR, and the CCM mappings to EU instruments such as ECUC give CSA-aligned organisations a documented control set that can serve as the foundation for an NCAF-aligned evidence pack. Where formal cross-mappings between CSA artefacts and the ENISA objectives have not yet been published, organisations should treat the alignment as a starting point for internal mapping work rather than as a turnkey crosswalk.

References

[1] ENISA. "Assess your National Cybersecurity Capabilities and Maturity with the updated ENISA Framework." ENISA News, April 22, 2026.

[2] ENISA. "National Capabilities Assessment Framework 2.0." ENISA Publications, April 22, 2026.

[3] ENISA. "National Cybersecurity Assessment Framework (NCAF) Tool." ENISA Topics, April 22, 2026.

[4] Industrial Cyber. "ENISA updates NCAF 2.0 to help governments measure and close cybersecurity gaps, push cyber maturity benchmarking." Industrial Cyber, April 23, 2026.

[5] NIS-2-Directive. "NIS 2 Directive Article 19: Peer Reviews." NIS 2 Directive Reference, accessed April 27, 2026.

[6] European Commission. "NIS2 Directive: securing network and information systems." Shaping Europe's Digital Future, accessed April 27, 2026.

[7] ENISA. "The EU Cybersecurity Index 2024." ENISA Publications, June 17, 2025.

[8] The Cyber Express. "Enhance EU Cybersecurity With NCAF 2.0 Framework." The Cyber Express, April 23, 2026.

[9] ENISA. "Multilayer Framework for Good Cybersecurity Practices for AI." ENISA Publications, accessed April 27, 2026.

[10] ENISA. "Cybersecurity of AI and Standardisation." ENISA Publications, March 14, 2023.

[11] ENISA. "National Capabilities Assessment Framework (full report, 2020)." ENISA Publications, December 2020.

[12] ENISA. "ENISA NIS360 2024 report: A comprehensive look at cybersecurity maturity and criticality of NIS2 sectors." ENISA News, March 5, 2025.

[13] Insight EU Monitoring. "ENISA releases new framework to assess National Cybersecurity Capabilities and Maturity." Insight EU Monitoring, April 22, 2026.

[14] NIS-2-Directive. "NIS 2 Directive Article 7: National Cybersecurity Strategy." NIS 2 Directive Reference, accessed April 27, 2026.

