

European cybersecurity certification in 2026

Key takeaways from the ENISA conference
and a workforce guide for NIS2 delivery.



➤

Executive Decision

Certification is becoming operational evidence.

The 2026 European Cybersecurity Certification Conference signalled a shift from policy design to evidence that buyers, regulators and providers can reuse. The direction is clear, but the system is not finished. EUCC is operating while EUMSS and EUDI Wallet certification remain candidate schemes. [1][3][4][5]

VERDICT Use certification, NIS2, ECSF and NICE as one operating system. Certification can strengthen assurance, but it does not replace accountable management, effective controls or competent people.

Decision lens	Strong case	Weak case
Compliance	NIS2 outcomes are mapped to controls, owners and evidence.	A certificate is treated as proof that every obligation is met.
Workforce	ECSF defines role coverage and NICE defines the work to perform.	Job titles stand in for tested capability and clear tasks.
Sourcing	An integrated team works in the client environment with named accountability.	Responsibility is pushed to a vendor and evidence is fragmented.

WHAT LEADERS SHOULD DO NEXT

- Map NIS2 and sector obligations to controls, evidence and management decisions.
- Map each control to accountable ECSF roles and to the tasks, knowledge and skills needed for delivery.
- Use product or service certification as supporting assurance, then test its scope against the actual risk.

PART 01

From policy to proof

01

The 2026 ENISA conference connected certification with the Cyber Resilience Act, NIS2 and EUDI Wallets. This part separates signal from status: what the conference actually said, and which schemes are adopted, candidate or still in draft.

The Conference	004
Key Takeaways	005
Scheme Status	006
Framework Connection	007

The Conference

Europe is moving from policy to proof.

ENISA held the 2026 European Cybersecurity Certification Conference on 15 April in Ayia Napa under the Cyprus Presidency of the Council of the EU. The programme connected certification with the Cyber Resilience Act, NIS2, EUDI Wallets and managed security services. It also put conformity assessment capacity on the agenda. [1]

01

Trust backbone

Certification is being positioned as reusable assurance.

02

Regulatory interplay

CRA and NIS2 increase demand for credible evidence.

03

New scheme scope

Services and organisational posture are entering the frame.

04

Capacity constraint

Assessment bodies may become a delivery bottleneck.

THE PRACTICAL READING

Conference thread	Operational consequence
From policy to proof	Create an evidence architecture that links controls, technical artefacts and decisions.
CSA2 proposal	Track the proposal separately from current law and avoid designing controls around unadopted text.
CRA and EUCC	Product teams need secure lifecycle evidence and a route to conformity assessment.
EUDI Wallet	Reusable component evidence and assurance composition will matter across supply chains.
EUMSS	Service buyers should define incident duties, integration boundaries and evidence access now.

JUDGEMENT The conference was not a signal to certify everything. It was a signal to decide where independent assurance reduces risk and where internal control evidence remains the better tool.

➤

Key Takeaways

Five signals for technology leaders.

The useful takeaways are less about individual certificates and more about how assurance will affect product, service and workforce decisions. [1][2][3]

Signal	What the evidence says	Leadership implication
1 Certification becomes reusable evidence	EU policy increasingly connects certification with regulatory and market assurance.	Design evidence once, but verify that scheme scope matches the obligation.
2 The scope is expanding	The revised framework covers ICT products, services, processes, managed security services and cyber posture.	Build a portfolio view of which assets or services warrant external assurance.
3 Product evidence rises in value	CRA implementation and EUCC increase attention on product security, lifecycle controls and assessment routes.	Bring engineering, security, legal and conformity planning together early.
4 Service trust becomes testable	The July 2026 EUMSS draft starts with an Incident Response service profile.	Write incident roles, hand-offs and evidence access into service design and contracts.
5 Capacity is part of the risk	The conference explicitly examined CAB and NAB availability for 2026 to 2028.	Reserve assessment capacity and do not place the entire timeline on a future certificate.

WHAT THIS DOES NOT MEAN

- Certification is not a substitute for NIS2 risk management, incident reporting or management oversight.
- An organisational ISO certificate is not proof that every engineer has the competence required for a role.
- A candidate scheme can shape planning, but requirements may change before adoption.

DECISION RULE Ask whether a certificate reduces duplicated assessment, strengthens market access or addresses a material assurance gap. If it does not, prioritise direct control evidence.



Scheme Status

Separate adopted schemes from candidate schemes.

Status is a decision variable. The value of a scheme depends on legal effect, market demand, assessment capacity and whether its scope matches the technology or service being bought. [3][4][5]

Scheme or policy	Status on 16 October 2026	Use now
EUCC	Adopted and operating since February 2025. The Commission reports 27 notified conformity assessment bodies and 16 certificates in the first transition year.	Use for relevant ICT products where Common Criteria assurance is proportionate.
EUMSS	Draft candidate scheme v1.1 published in July 2026. ENISA lists 13 September 2026 as the response deadline, although the page still labels the review ongoing.	Use as a design signal for managed security service requirements, not as an available EU certificate.
EUDI Wallet	Candidate scheme under development and public review in 2026.	Plan for component evidence, assurance composition and national implementation dependencies.
NIS2	In force through national transposition. Targeted EU amendments were proposed in January 2026.	Use current national law and sector guidance. Track proposed changes separately.
ECSF	Current 12-profile framework. ENISA is revising it and plans consultation at the end of 2026.	Version the role catalogue so future proficiency levels can be incorporated cleanly.

STATUS DISCIPLINE A draft can be useful for readiness, but it must not be described as an adopted certification obligation. Keep a legal register that distinguishes current law, proposed amendments, candidate schemes and voluntary practice.

CERTIFICATION OBJECT MATTERS

Product and service schemes assess a defined object and assurance level. ECSF and NICE describe workforce capability. NIS2 defines organisational outcomes and accountability. Treating these as interchangeable weakens the evidence chain.

Framework Connection

Connect obligations to people and work.

The frameworks are complementary. A useful operating model starts with the required outcome, assigns accountable roles, defines observable work and records evidence. [6] [7][8][9]

NIS2	ECSF	NICE	EU schemes
Required outcomes	Role profiles	Work definition	Assurance evidence
Risk measures, reporting and management accountability.	A common EU language for responsibilities and competence.	Work Roles, Competency Areas and task, knowledge and skill statements.	Independent evidence for a defined product or service scope.

USE EACH TOOL FOR THE QUESTION IT ANSWERS

Question	Primary tool	Expected output
What must the organisation achieve	NIS2 plus national and sector rules	Obligation, accountable owner, deadline and evidence need
Who must own or perform the work	ECSF	Role profile, responsibilities and capability coverage
What work must be observable	NICE	Tasks, knowledge, skills, competency areas and work-role assignments
What independent assurance is useful	EU certification scheme	Certificate scope, assurance level, dependencies and validity

PRACTICAL RULE Start with the obligation and evidence need, not a job title, a certificate or a supplier catalogue. ENISA already maps NIS2 obligations to ECSF roles, and NICE adds task-level precision (components at version 2.2.0 as of 28 April 2025); maintain the resulting crosswalk as a controlled artefact as the schemes continue to evolve.

PART 02

From roles to delivery

NIS2, ECSF and NICE describe outcomes, roles and work. This part turns that framework into a workforce blueprint and a clear accountability model for an integrated team.

Workforce Blueprint	009
Operating Model	010
Nearshore Portugal Fit	011

➤

Workforce Blueprint

Build capability around NIS2 outcomes.

The table is a practical blueprint, not an official ECSF to NICE crosswalk. It shows how leaders can turn regulatory outcomes into team design and evidence. [8][9]

NIS2 outcome area	Indicative ECSF coverage	NICE-style work definition	Evidence to retain
Governance and risk	CISO, Cybersecurity Risk Manager, Cyber Legal, Policy and Compliance Officer	Maintain risk register, advise management, approve treatment and track exceptions.	Minutes, decisions, risk acceptance, control ownership and metrics
Incident handling	Cyber Incident Responder, Digital Forensics Investigator	Triage, contain, escalate, preserve evidence and coordinate reporting.	Runbooks, case records, timestamps, lessons learned and reporting log
Supply chain security	Risk Manager, Cybersecurity Architect, Auditor	Assess suppliers, define security requirements and monitor dependencies.	Due diligence, contract clauses, architecture evidence and remediation
Secure development	Cybersecurity Architect, Implementer, Penetration Tester	Threat model, implement secure controls, test and manage vulnerabilities.	Design decisions, test results, SBOM, fixes and release approval
Business continuity	CISO, Incident Responder, Risk Manager	Define recovery priorities, exercise scenarios and improve resilience.	BIA, plans, exercise results, recovery tests and improvement actions

COMPETENCE TEST For every critical task, identify a primary performer, a reviewer, the required knowledge, the evidence of competence and the evidence produced by the work.

AVOID TITLE INFLATION

A person can hold a senior title without covering the required tasks. Assess teams against observable work and decision rights, then use professional certifications as supporting evidence where they are relevant.

Operating Model

Keep accountability inside the organisation.

NIS2 brings cybersecurity into the boardroom and assigns management accountability. A nearshore model can expand execution capacity, but it cannot transfer the client’s legal accountability or risk acceptance. [6]

Client retains	Shared design and control	Nearshore team can execute
Management approval and oversight	Capability model and RACI	Engineering and operational tasks
Risk appetite and risk acceptance	Control design and evidence standards	Control implementation and documentation
Regulatory interpretation and notification decisions	Incident thresholds, escalation and exercises	Monitoring, triage, containment support and records
Supplier selection and assurance decisions	Due diligence, service levels and remediation	Technical assessments and evidence collection
Strategic architecture and exceptions	Secure design reviews and delivery guardrails	Threat modelling, testing, fixes and release evidence

FOUR CONTROLS FOR AN INTEGRATED TEAM

- Named people with stable role assignments, deputies and explicit escalation routes.
- Work performed in the client backlog, tooling, access model and evidence repository.
- Client-owned definitions of done for security, testing, documentation and handover.
- Regular capability reviews against the ECSF role map and NICE-style task catalogue.

RED FLAG If the supplier controls the evidence, chooses what to report and owns the only working knowledge of the system, the client has created an assurance dependency rather than resilience.

➤

Nearshore Portugal Fit

Nearshore Portugal fits the evidence-led team model.

The strongest fit is not generic staff augmentation. It is an EU-based integrated team built around explicit roles, client-owned controls and continuity of delivery. Nearshore Portugal’s operating model is designed for that combination. [11][12]

What the buyer needs	How Nearshore Portugal fits	What to verify in the engagement
Role-level precision	Curated profiles can be aligned to ECSF responsibilities and a task catalogue.	Named role coverage, task evidence and interview criteria
Integrated delivery	Engineers work in the client’s tools, processes and culture.	Access controls, repositories, review gates and definition of done
EU operating context	Portugal supports time-zone overlap and delivery within EU legal frameworks.	Data locations, subcontractors, incident routes and contract scope
Continuity and scale	Dedicated teams and nearshore hubs support stable capability rather than isolated placements.	Retention, succession, ramp-up, knowledge transfer and exit readiness

COMPANY-REPORTED DELIVERY BENCHMARKS

24 to 72h

CV turnaround

After scope alignment

4 to 8 wks

Team ramp-up

For an operating team

85 to 95%

Retention

Reported continuity range



Sources

Primary sources.

[1](#) ENISA 2026 European Cybersecurity Certification Conference

[3](#) European Commission European cybersecurity certification framework

[5](#) ENISA draft candidate EUDI Wallet scheme

[7](#) ENISA European Cybersecurity Skills Framework

[9](#) NIST NICE Framework current versions

[11](#) Nearshore Portugal company and operating benchmarks

[13](#) European Commission CRA conference slides

[2](#) European Commission CSA2 proposal conference slides

[4](#) ENISA draft candidate EUMSS Scheme v1.1

[6](#) European Commission NIS2 Directive overview

[8](#) ENISA cybersecurity roles and skills for NIS2 entities

[10](#) ENISA NIS Investments 2025

[12](#) Nearshore Portugal delivery process

[14](#) ENISA EUMSS conference slides

From policy to proof

Build the evidence, capability and delivery
model together.

nearshoreportugal.com
info@nearshoreportugal.com