



ShieldNet

Document Title	ShieldNet Cybersecurity Standard – Annex C – Certification Schema
Release Date	September 2025
Approved by	<i>[Pending Approval]</i>
Next Review	August 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0

1. Why the Certification Program Exists

The ShieldNet Certification Program is here to give organizations a clear, credible way to show they meet the ShieldNet Cybersecurity Standard. It's designed for SMEs, NGOs, and startups that want to prove they are serious about security — without getting lost in the paperwork and high costs of traditional certifications like ISO 27001.

The program awards compliance badges to organizations that put the ShieldNet controls into action and can show real evidence that they're meeting both the core EU-wide cybersecurity obligations and, if relevant, any sector-specific add-ons. These badges are easy to understand for customers, partners, and regulators, and they provide a quick trust signal in the marketplace.

Whether you're a new ShieldNet member starting with the basics or a mature organization managing advanced risks, the certification program gives you a roadmap for where you stand today and how to level up over time. The goal is simple: help you prove your compliance, build trust, and compete with confidence in the EU's digital economy.

2. Badge Levels & What They Mean

The ShieldNet Certification Program offers three badge levels that reflect increasing depth of assurance. Each level builds on the ShieldNet Core Standard's 48 controls and uses the Annex A templates as primary evidence. You can certify an entire organization or a specific product/service (define the scope up front). A Sector Add-On can be layered onto any level.

2.1. Level 1 — Starter (Core Compliant)

Who it's for: Small teams getting their baseline in place, or organizations needing a fast, credible trust signal.

What it proves: You've implemented the 48 core controls and keep the Core Templates (A-1 to A-6) up to date.

Evidence & review

- Self-assessment checklist covering all 48 controls.
- Sample evidence pack: A-1, A-2, A-3, A-4 for the last 90 days; A-5 and A-6 current.
- Desk review by an accredited reviewer (no on-site interviews).

Passing criteria

- All 48 controls implemented (can be light-weight), 0 major gaps, ≤5 minor gaps with a 60-day fix plan.

Validity & upkeep

- 12 months; light mid-cycle check optional.
- Badge can be renewed with updated templates + closure of past minors.

2.2. Level 2 — Verified (Independently Reviewed)

Who it's for: Organizations that want third-party validation of implementation and basic effectiveness.

What it proves: Controls are not only in place but are working in practice across a representative sample of systems and suppliers.

Evidence & review

- All Core Templates (A-1 to A-6) current; at least two Extended Templates in use (e.g., A-8 Access Reviews, A-9 Vulnerabilities).
- Independent review with document sampling, interviews (Info-Sec Coordinator, a system owner, and one business lead), and configuration spot-checks (e.g., MFA, backups).
- Optional lightweight technical test (e.g., authenticated vuln scan).

Passing criteria

- ≥ 90% of applicable controls evidenced as effective in sample; 0 major gaps; ≤3 minor gaps with a 45-day fix plan.

Validity & upkeep

- 24 months with a 12-month surveillance check (mini-update of A-1/A-2/A-9 and incident summary).

2.3. Level 3 — Assured (Advanced Audit)

Who it's for: Organizations with higher risk exposure, larger customer commitments, or those seeking ISO-like assurance without the bureaucracy.

What it proves: Controls are systematically implemented and effective, with metrics, testing, and continuous improvement in place.

Evidence & review

- Core Templates current + at least four Extended Templates (A-7 legal mapping, A-8 access reviews, A-9 vuln & patch log, A-10 policy reviews, A-11 KPIs, A-13 BC/DR tests as applicable).

- Comprehensive audit: document review, wider interviews, technical verification (config checks, representative vulnerability scans, restore tests evidence), and tabletop incident/BCP exercise.

Passing criteria

- 100% of applicable controls implemented; $\geq 85\%$ effectiveness demonstrated across samples; 0 major gaps; ≤ 2 minor gaps closed within 30 days.

Validity & upkeep

- 36 months with annual surveillance (targeted re-sampling and KPI review).

2.4. Sector Add-On (Optional, Any Level)

What it is: A focused pack of sector-specific controls and obligations that sit on top of your base level (e.g., healthcare, finance, energy, high-risk AI).

How it works:

- Select the relevant sector pack; Annex B's Extensive Matrix maps obligations to add-on controls.
- Assessment is bundled into your chosen level (Starter/Verified/Assured).
- Validity: same as your base badge; sector scope listed on the certificate (e.g., "Verified Healthcare").

2.5. Badge Use & Revocation (All Levels)

This section sets the rules for displaying your certification badge and the circumstances where it can be suspended or withdrawn.

- Badges may be displayed on websites, proposals, and job posts only with the correct level and scope.
- Misuse (wrong level/scope, expired badge) or material security failures (e.g., willful non-disclosure) can trigger suspension or revocation.
- Organizations must promptly disclose significant scope changes (e.g., major new product or acquisition) — a scope update may be required.

3. How To Receive a Badge

The ShieldNet Certification assessment is designed to be practical, transparent, and proportionate to your organization's size, risk level, and chosen badge tier. While the depth of testing increases with each level, the overall process follows the same four stages: Application & Scope Definition, Evidence Preparation, Independent Review, and Decision & Badge Issuance.

3.1. Application & Scope Definition

Every certification journey starts with defining exactly what will be assessed. You can certify your entire organization or a specific product/service.

- Scope boundaries are clearly documented: physical locations, teams, products, and systems included.
- Any exclusions must be justified (e.g., legacy systems being phased out).
- For Sector Add-Ons, the scope must also confirm which sector obligations apply.

A defined scope ensures the review is focused, prevents scope creep, and makes your badge accurate and credible.

3.2. Evidence Preparation

Once scope is agreed, you gather and organize the evidence needed for your chosen badge level:

- Core Templates (A-1 to A-6) are always required.
- Extended Templates (A-7 to A-13) are required in part or in full depending on level:
 - Starter: Core Templates only
 - Verified: Core Templates + at least 2 Extended Templates
 - Assured: Core Templates + at least 4 Extended Templates
- Evidence must be current — for example, risk assessments within the last 12 months, incident logs up to the present month.

Tip: Maintain these artefacts regularly (Annex A guidance) so you can submit without last-minute stress.

3.3. Independent Review

During the independent review, an accredited assessor examines your evidence, interviews key staff, and, depending on the badge level, performs technical checks to verify that controls are effective in practice. The review process varies by badge level:

- Starter: Desk-based evidence review by an accredited assessor. No live interviews, but clarifications may be requested.
- Verified: Desk review + targeted interviews with key staff (Info-Sec Coordinator, one system owner, one business lead) + spot checks of technical settings (e.g., MFA enabled).
- Assured: Full evidence review + expanded interviews across departments + technical verification (representative vulnerability scans, restore test results, tabletop incident drill).

Reviews check both implementation and effectiveness. Effectiveness means the control isn't just "there" — it works as intended in day-to-day operations.

3.4. Decision & Badge Issuance

This stage finalizes your certification, confirming whether you meet the required standard and awarding your badge once any identified gaps are addressed.

After the review:

- The assessor compiles a findings report detailing compliance status, any major or minor gaps, and recommended improvements.
- Major gaps must be resolved before certification can be granted.
- Minor gaps can be certified with a remediation plan, provided they are closed within the set time window (60/45/30 days depending on level).
- Once approved, you receive a digital certificate and badge for your chosen level and scope.

The certificate lists:

- Organization name
- Certification level (and sector add-on if applicable)
- Scope statement (entity, products, locations)
- Date of certification and valid-until date
- Assessment body name

4. Visual Identification

4.1. Square ShieldNet Certification Badge



Level 1 – Starter Badge



Level 2 – Verified Badge



Level 3 – Assured Badge

4.2. Rectangular ShieldNet Certification Badge



ShieldNet
Certified - Starter

Level 1 – Certified Starter Badge



ShieldNet
Certified - Verified

Level 2 - Certified Verified Badge



ShieldNet
Certified - Assured

Level 3 – Certified Assured Badge

5. Outro

Earning a ShieldNet certification badge is more than just a compliance exercise — it's a public commitment to responsible cybersecurity practices. Whether you start at the Starter, Verified, or Assured level, your badge sends a clear message to customers, partners, and regulators that your organization is serious about protecting data, meeting EU legal obligations, and operating securely in the digital economy.

Certification is also a roadmap for growth. The Core and Extended Templates in Annex A, combined with the legal mapping in Annex B, give you a practical structure for keeping your controls effective year-round. As your organization evolves, you can move up badge levels or add sector-specific compliance packs to meet new demands without overhauling your entire approach.

Finally, the ShieldNet certification program is designed to stay relevant as technology, threats, and laws change. Regular reviews, surveillance checks, and renewal cycles ensure your badge reflects your current security posture, not just a point in time. By maintaining your certification, you not only keep your legal footing but also strengthen your reputation as a trusted, resilient, and competitive player in the EU's connected marketplace.