



ShieldNet

Document Title	ShieldNet Cybersecurity Standard – Annex D – Education Schema
Release Date	March 2026
Next Review	February 2027 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0

1. Why this Education Schema Exists

Cybersecurity maturity is not achieved only by installing tools or writing policies. It depends on people who understand their responsibilities, can interpret controls correctly, and can apply them proportionately within an SME environment. Without structured competence development, even well designed controls become symbolic rather than effective.

This Education Schema exists to ensure that ShieldNet implementation is supported by structured, role based, and operationally relevant education. Certification without competence is ineffective. An organization may possess templates and badges, but without trained Implementors, informed Board oversight, capable System Owners, and independent Auditors, the system will not function as intended.

This Annex complements the Core Standard and the Cybersecurity Management System by defining qualification pathways and competence expectations. It supports SMEs, NGOs, and startups that lack large internal security teams by providing clear learning streams aligned to real operational needs. It also strengthens certification readiness by ensuring that those implementing or auditing ShieldNet have demonstrated knowledge and practical capability.

2. Structure of the Education Schema

Annex D is divided into two major parts that address different dimensions of cybersecurity competence.

2.1. Role Based Qualification Path

This section focuses on governance and management system roles. It defines the education, assessment, and renewal requirements for professionals who implement and audit the ShieldNet Cybersecurity Management System.

2.2. Competence Streams aligned to ECSF

This section focuses on operational cybersecurity capability across technical and governance domains. It maps learning streams to practical career tracks aligned to the European Cybersecurity Skills Framework and to ShieldNet Action Zones.

Both parts are complementary but distinct. The Role Based Qualification Path ensures the integrity of the management system and certification process. The Competence Streams ensure that operational security functions are capable and sustainable. Core Training is mandatory and foundational for both.

3. Role Based Qualification Path Management System Roles

This section defines formal education requirements for two specific roles within the ShieldNet ecosystem:

- Implementor
- Auditor

These roles relate specifically to implementing and auditing the ShieldNet Cybersecurity Management System and Core Standard. They do not replace internal roles such as Board, Info Sec Coordinator, System Owner, or Third Party Provider. Instead, they support organizations in applying and validating the framework correctly..

3.1. Implementor

Implementor: expert responsible for implementing the ShieldNet Cybersecurity Management System and ensuring controls are operational and evidenced.

Purpose of the Role:

The Implementor supports SMEs in translating the 48 controls and Action Zones into structured Objectives and Key Results. This role ensures that controls are not only documented, but actively implemented, measured, and evidenced using Annex A artefacts. For small organizations without internal GRC maturity, the Implementor provides structure, proportionality, and practical guidance.

Core Competence Areas

An Implementor must demonstrate capability in the following areas:

- Understanding of ShieldNet Core Standard structure and the five Action Zones
- Ability to operationalize controls into measurable OKRs
- Ability to manage and structure Annex A artefacts as evidence
- Risk assessment methodology aligned to SME proportionality
- Governance cadence facilitation with Board and Info Sec Coordinator
- Evidence management and traceability across controls and artefacts
- SME proportionality judgment when applying controls

Required Knowledge Domains

The Implementor must possess foundational knowledge in:

- EU cybersecurity regulatory baseline awareness
- Risk management fundamentals
- Access control and vulnerability governance basics

- Incident handling fundamentals
- Continuous improvement principles

Training Requirements:

To qualify as an Implementor, the following must be completed:

- Mandatory Core Training
- Implementor Professional Training program
- Practical case based implementation workshop using simulated SME scenario
- Formal assessment combining knowledge test and scenario evaluation

Certification Validity and Renewal:

- Validity period: 3 years
- Minimum Continuing Professional Development hours per year
- Evidence of at least one completed ShieldNet implementation or equivalent supervised engagement
- Renewal assessment or peer review validation.

3.2. Auditor

Auditor: expert responsible for independently evaluating conformity of the organization against the ShieldNet Core Standard and Cybersecurity Management System.

Purpose of the Role

The Auditor provides independent assurance that controls are implemented and effective. This role strengthens trust within the ShieldNet certification model and ensures that badge levels reflect real operational capability. Independence and objectivity are central to this function.

Core Competence Areas

An Auditor must demonstrate competence in:

- Control interpretation and intent analysis
- Evidence sufficiency evaluation
- Interview techniques for Board, Info Sec Coordinator, and System Owners
- Sampling methodology appropriate for SMEs
- Gap classification using major and minor findings
- Risk based judgment and proportionality
- Clear and structured reporting

Required Knowledge Domains

The Auditor must understand:

- Annex C certification levels and assurance expectations
- Annex A artefact sufficiency and effectiveness criteria
- Audit ethics and independence principles
- Basic technical verification capability including configuration checks and vulnerability report interpretation

Training Requirements

To qualify as an Auditor, the following must be completed:

- Mandatory Core Training
- Auditor Professional Training program
- Participation in at least one supervised audit engagement
- Formal written and practical assessment

Independence and Ethics Requirements

Auditors must adhere to strict independence standards:

- No auditing of own implementation work
- Mandatory conflict of interest declaration before each engagement
- Confidentiality obligations regarding client information

Certification Validity and Renewal

- Validity period: 3 years
- Participation in surveillance or peer review activities
- Minimum annual continuing education hours in cybersecurity or audit domains.

4. Competence Streams aligned to ECSF

This section maps operational training streams to practical cybersecurity career tracks aligned to the European Cybersecurity Skills Framework. These streams are not limited to ShieldNet implementation. They support real operational capability within SMEs and strengthen long term workforce resilience. Each stream includes two advanced progression tiers: Advanced and Professional, built on a foundational level.

4.1. Blue Team and Operations

Purpose

This stream supports operational defense functions including detection, response, monitoring, patching, and resilience testing. It strengthens the WATCH AND PATCH and REACT AND RECOVER Action Zones.

Target Audience

- Info Sec Coordinator
- System Owner
- Technical staff responsible for monitoring and patching

Core Competence Areas

- Log analysis and alert interpretation
- Vulnerability management lifecycle
- Incident response procedures
- Backup validation and restore testing
- Endpoint security configuration
- Threat awareness and intelligence consumption

Action Zone Mapping

- WATCH AND PATCH
- REACT AND RECOVER

Progression Levels

- Foundation – basic monitoring and patch execution
- Practitioner – coordinated incident handling and vulnerability governance
- Advanced – structured detection capability and resilience testing

4.2. Build and Product Security

Purpose

This stream supports secure development and secure architecture practices. It strengthens SHIELD AND BUILD and KNOW AND PLAN Action Zones, particularly where digital products or AI systems are involved.

Target Audience

- Developers
- DevOps engineers
- Product Owners
- System Owners

Core Competence Areas

- Secure coding principles
- Secure configuration baselines
- Threat modeling methodology
- AI system risk awareness
- Encryption fundamentals
- DevSecOps integration practices

Action Zone Mapping

- SHIELD AND BUILD
- KNOW AND PLAN

Progression Levels

- Foundation – secure coding hygiene and configuration awareness
- Practitioner – structured secure development lifecycle integration
- Advanced – architecture level risk analysis and control integration

4.3. GRC Risk and Audit

Purpose

This stream supports governance, legal mapping, risk management, compliance monitoring, and assurance functions. It strengthens KNOW AND PLAN and LEARN AND LIFT Action Zones.

Target Audience

- Info Sec Coordinator
- Implementor candidates
- Auditor candidates
- Compliance or legal staff

Core Competence Areas

- Risk assessment methodology
- Legal mapping to controls
- Control design and documentation
- KPI development and metrics tracking
- Internal audit techniques
- Supplier governance

Action Zone Mapping

- KNOW AND PLAN
- LEARN AND LIFT

Progression Levels

- Foundation – basic risk register and compliance awareness
- Practitioner – structured governance reporting and audit participation
- Professional – independent assessment and strategic advisory capability

5. Core Training Free Self-Paced Program

Core Training is the foundational, free, self-paced digital program available to everyone. It establishes a shared language and understanding of the framework before advanced qualifications are pursued.

Core Training introduces:

- Understanding of the digital world
- Concepts of attackers and their weapons
- Practical protection mechanisms
- Capabilities to respond to incidents
- Security habits and culture

Target Audience

- Everyone regardless of their age, profession and technological knowledge

Program Structure

- Estimated duration: 3 to 5 hours total
- Modular online format
- Short knowledge checks after each Action Zone

Assessment and Evidence

- Final multiple choice assessment

- Digital completion certificate

6. Learning Progression Model

ShieldNet uses a simple four stage learning progression suitable for SMEs.

- Awareness – understands terminology and basic responsibilities
- Practitioner – can apply controls within daily role
- Professional – can design, assess, and improve systems
- Expert – can implement or audit independently

SMEs can scale training proportionally. A micro organization may require only Awareness across staff and one Practitioner level Info Sec Coordinator. A growing SME may require Professional level Implementor support and Advanced Blue Team capability. The model allows incremental maturity without overwhelming resource requirements.

7. Governance of the Education Schema

The Education Schema must remain aligned with the evolving Core Standard and certification expectations. Governance ensures consistency, quality, and relevance.

Curriculum Ownership

- Owned by ShieldNet governance body
- Supported by certified Implementors and Auditors

Review Cycle

- Annual review aligned to Core Standard update cycle
- Immediate update if Annex C certification levels change

Alignment Requirements

- Maintain terminology consistency with Core Standard
- Reflect updates in Annex A artefact expectations
- Align assessment depth with certification badge levels

Version Control

- Each training module version documented
- Change log maintained
- Previous versions archived for traceability

8. Alignment with Certification and Community Model

Education strengthens certification credibility. Training supports certification levels defined in Annex C and prepares organizations for Starter, Verified, and Assured assessments.

Implementors support structured adoption within SMEs and improve first time certification success. Auditors support trust by ensuring independence and consistent evaluation.

Operational streams build workforce capacity across Blue Team, Build and Product Security, and GRC domains. This reduces dependence on external frameworks and supports development of a structured European alternative tailored to SMEs.

By combining Core Training, role based qualifications, and operational streams, Annex D ensures that ShieldNet is not only a standard of documentation, but a structured competence ecosystem that sustains cybersecurity maturity over time.