MODULAR COMPLIANCE

Daniel Thompson-Yvetot

MODULAR COMPLIANCE

Daniel Thompson-Yvetot

ETSI Special Rapporteur
OSS Maintainer
Entrepreneur & Author

Talk Overview

What do we want? To make a Declaration of Conformity.

How do we get it? Assessment + Retention of Evidence

How do we do it? Choose Your (Presumption of) Conformity Pathway:

a. DIY, Harmonised Standard or Bespoke (Modules A, B+C, H)
b. EUCC for Product + CSA2 for Process
c. Common Specification (Only if things go wrong with harmonized standards)

When can we do it? Soon™ (After notification of CABs)

Presumption of Conformity (1/3)

Legal effect: When a product benefits from presumption of conformity, it is legally presumed to meet the essential cybersecurity requirements (Annex I) without the manufacturer needing to demonstrate compliance through additional evidence or assessment for those specific requirements

Partial coverage: Presumption applies only "insofar as" the standard, common specification, or certification scheme covers the specific essential requirements in question. If a harmonised standard only addresses some requirements, the manufacturer must still demonstrate conformity with the uncovered requirements through other means

Three pathways to presumption (Article 27):

- Harmonised standards with references published in the OJEU
- Common specifications adopted by Commission implementing acts (fallback when standards are absent or insufficient)
- European cybersecurity certification schemes under the Cybersecurity Act (2019/881)

Presumption of Conformity (2/3)

Article 27(1) - Harmonised standards

Products conforming to harmonised standards (references published in the OJEU) are presumed to meet the essential cybersecurity requirements covered by those standards

Article 27(2)-(4) - Common specifications (Backdoor)

- Where harmonised standards do not exist or are insufficient, the Commission may adopt implementing acts establishing common specifications
- Article 27(5) grants presumption of conformity for products meeting these common specifications

Article 27(8) - European cybersecurity certification schemes (like **EUCC** for Product)

- Products with an EU statement of conformity or certificate issued under a European cybersecurity certification scheme adopted pursuant to **Regulation (EU) 2019/881** (the Cybersecurity Act) are presumed to conform to the essential requirements covered by that certificate

Article 27(9) - Delegated acts specifying which schemes apply (like **CSA2** for Processes)

- Empowers the Commission to adopt delegated acts specifying which European cybersecurity certification schemes (under the Cybersecurity Act) can be used to demonstrate CRA conformity

Presumption of Conformity (3/3)

Does not eliminate conformity assessment: Presumption of conformity addresses the substantive question of whether requirements are met. The procedural question of which conformity assessment module applies (A, B+C, or H) remains determined by Article 32 and the product classification

Practical significance for Important Class I products: Under Article 32(2), if a manufacturer of an Important Class I product fully applies harmonised standards (or common specifications, or holds a relevant EU cybersecurity certificate), they may use self-assessment (Module A). Without presumption of conformity, they must use third-party assessment (B+C or H)

Module A - Internal Control

What it is

- Self-assessment by manufacturer alone
- No third-party (notified body) involvement
- Manufacturer bears full responsibility for conformity

Manufacturer obligations

- Draw up technical documentation (Annex VII)
- Ensure design, development, production and vulnerability handling comply with Annex I
- Affix CE marking and issue EU declaration of conformity

When it applies under CRA

- All default products (regardless of standards applied)
- Important Class I products only if harmonised standards, common specifications, or EU cybersecurity certification fully applied
- Not available for Important Class II or Critical products

Module B - EU-Type Examination

What it is

- Third-party examination of a product type by a notified body (CAB)
- First stage of a two-part process (must be followed by Module C)

What gets examined

- Technical design and development of the product
- Vulnerability handling processes
- Specimens of critical product parts

Output

- EU-type examination certificate (valid up to 5 years, renewable)
- Attests the type meets essential cybersecurity requirements
- Must be retained 10 years or support period, whichever longer

Key limitation

- Validates design only, not ongoing production
- Cannot be used standalone under CRA

Module C - Conformity to Type (Internal Production Control)

What it is

- Second stage following Module B
- Together: third-party validated design + efficient internal production
- Internal manufacturer process ensuring all products match the certified type

Manufacturer obligations

- Ensure manufacturing produces products conforming to approved type
- Affix CE marking to each conforming product
- Draw up EU declaration of conformity

When B+C applies under CRA

- Important Class I without full harmonised standards
- All Important Class II products
- Critical products (if no EU cybersecurity certification scheme available)

Module H - Full Quality Assurance

What it is

- Third-party assessment of manufacturer's quality management system
- Covers design, development, production, and vulnerability handling processes
- Alternative to Module B+C (and A!)

Notified body role

- Audits and approves the quality system
- Inspects one product according to method
- Conducts periodic surveillance (minimum every 12 months)
- May perform unannounced visits

Quality system must document

- Quality objectives and organisational structure
- Design and production control techniques
- Testing procedures (before, during, after production)
- Inspection reports, test data, calibration records

EUCC - EU Common Criteria Certification

What it is

- European cybersecurity certification scheme under Cybersecurity Act (2019/881)
- Based on Common Criteria (ISO/IEC 15408)
- Adopted 31 January 2024, first certificates from February 2025

Who performs it

- ITSEFs (IT Security Evaluation Facilities) conduct product evaluation
- Certification Bodies issue the certificate
- Both are CABs accredited under the Cybersecurity Act framework

CRA relevance (Article 27(8)-(9))

- Products with EUCC certificate presumed to conform to covered Annex I requirements
- Requires "substantial" or "high" assurance level
- Commission delegated acts will formally specify CRA presumption of conformity