EUROSMART

The Voice of the Digital Security Industry

Full Quality Assurance for CRA Conformity Assessment

Implementing Module H under the CRA

Philippe Proust
Security Director, Thales Group

Pierre-Jean Verrando
Director General, Eurosmart

1. Conformity Assessment under the CRA

Manufacturers may demonstrate compliance through several procedures depending on PwDE classification.

- **Module A - Internal control**
- manufacturer self-assessment

- **Module B + C - EU-type examination**
- product type evaluated by a third party

- **Module H - Full Quality Assurance**
- evaluation of the **manufacturer's quality management system**

Module H ensures that the **processes used to develop and maintain products consistently produce compliant products**.

2. Benefits of Module H (Full Quality Assurance)

Process-Based Conformity Assessment

Module H focuses on the **manufacturer's Quality Assurance System** rather than testing every product individually.

Meaning that:

- cybersecurity is integrated into **organizational and development processes**
- compliance is ensured **throughout the development lifecycle**
- products developed under the certified system are expected to meet CRA requirements.

Benefits: **more scalable for manufacturers with multiple products**

- streamline the compliance process for multiple products
- promote consistency & standardization across product lines
- optimize audits by Notified Bodies

3. Module H: Full Quality Assurance

Module H focuses on assessing the processes implemented by the manufacturer

Key characteristics:

- implementation of a **Quality Assurance System**
- integration of cybersecurity into **design, development and production**
- certification by a **notified body**
- continuous **surveillance audits**

Module H may also reuse results from previously certified products or existing certification schemes, reducing duplication of conformity assessments.

- ➢ EUCC evaluation results could potentially be reused for Module H conformity assessment under the CRA, but this would require formal recognition - typically through a delegated act - to establish **presumption of conformity**
- ➢ Without such recognition, reuse **remains possible only as supporting evidence**, not as **automatic proof of conformity**.

4. No hEN available or not suitable? Compliance is still possible!

Under the **CRA** manufacturers **may** demonstrate compliance with the essential cybersecurity requirements by applying **harmonised European standards (hEN)**.

When a product complies with a harmonised standard cited in the **Official Journal of the European Union**, it benefits from **presumption of conformity** with the relevant CRA requirements.

Benefits of harmonised standards:

- provide **technical specifications for security requirements**
- simplify conformity assessment
- ensure **consistent implementation across the EU market**

But not mandatory for Module H – class II and critical product

For class I products, compliance with harmonized standards enables module A (self assessment)

For class II and critical products, compliance with a harmonized standard must be assessed by a Notified Body

5. Full Quality Assurance System - QAS - for Products

To demonstrate compliance under Module H, the manufacturer must implement a **Quality Assurance System covering product cybersecurity**.

1. Manufacturer responsibilities

In addition to its legacy QAS, the manufacturer must:

- define **cybersecurity policies and governance structures**
- implement **risk management processes**
- integrate cybersecurity into **product development and operational processes**
- maintain **documentation demonstrating compliance**

The QAS must ensure that all products developed under this framework meet the **CRA essential cybersecurity requirements**.

5. Full Quality Assurance System - QAS - for Products

2. Notified Body responsibilities

The notified body must:

- evaluate the **design and implementation of the manufacturer’s Quality Assurance System**
- verify that processes address CRA requirements
- assess whether the system can **consistently produce compliant products**
- approve the system before certification.

The Notified Body can rely on a certified QAS (e.g. ISO 9001) and on outcomes of audits of the Quality Assurance System as applied at product level

6. Scope of the Full Quality Assurance System

The scope of the Full Quality Assurance System must include **all processes related to products with digital elements**.

1. Manufacturer responsibilities

The manufacturer must ensure that the management system covers:

- **Product lifecycle processes**
  - product design
  - software development
  - Production

- **Operational lifecycle processes**
  - vulnerability handling
  - security updates
  - maintenance during the support period

- **Remote Data Processing Services** If the product depends on remote services (e.g. cloud, backend infrastructure), the manufacturer must ensure that:
  - these services are included in the **security processes**
  - vulnerabilities affecting these services are managed
  - updates and security monitoring are implemented.

6. Scope of the Full Quality Assurance System

2. Notified Body responsibilities

The notified body must verify that:

- the **scope of the Quality Assurance System is correctly defined**
- all relevant product and service components are included
- remote services necessary for product functionality are covered by security processes.

7. Cybersecurity Risk Assessment

1. Manufacturer responsibilities

The manufacturer must perform a **cybersecurity risk assessment** for products with digital elements.

This includes:

- identifying cybersecurity threats and vulnerabilities
- assessing risks to **confidentiality, integrity and availability**
- considering the **intended use and reasonably foreseeable misuse** of the product
- evaluating potential impacts on **users and other affected parties**
- defining appropriate **risk treatment measures**
- The risk assessment determines the **security controls and technical measures required to meet CRA essential cybersecurity requirements**.

7. Cybersecurity Risk Assessment

2. Notified Body responsibilities

The notified body must verify that:

- the manufacturer has implemented a **structured risk assessment process**
- risk acceptance criteria are defined
- risks affecting users and regulatory compliance are addressed
- the selected security controls correspond to the **identified risks**.

8. Secure Development Lifecycle

1. Manufacturer responsibilities

The manufacturer must integrate cybersecurity into the **design, development and production processes**.

This includes:

- **Design phase**
  - defining security requirements
  - performing product-specific cybersecurity risk assessments
  - designing secure system architecture
- **Development phase**
  - applying secure coding practices
  - integrating security controls
- **Verification phase**
  - conducting security testing
  - performing vulnerability scanning
  - carrying out penetration testing where appropriate

Products must not be placed on the market **until security requirements have been verified**.

8. Secure Development Lifecycle

2. Notified Body responsibilities

The notified body must verify that:

- secure development processes are implemented
- security checkpoints exist before product release
- testing and verification activities are adequate
- development processes address the **essential cybersecurity requirements defined in CRA Annex I**.

9. Vulnerability Handling Requirements

Sources

Vulnerability handling requirements originate from CRA Annex I Part II and are implemented using reference to international standards like ISO 29147 and ISO 30111.

1. Manufacturer Responsibilities

The manufacturer must implement a **structured vulnerability handling process**, including:

- identification and documentation of vulnerabilities
- maintenance of information on software components (e.g. SBOM)
- regular security reviews
- remediation of vulnerabilities **without undue delay (based on the manufacturer's risk assessment)**
- distribution of **security updates and patches**
- implementation of a **coordinated vulnerability disclosure policy**
- reporting **actively exploited vulnerabilities and incidents** to the competent authority/ENISA where required

These processes must operate throughout the **defined support period of the product (starts when the PwDE is placed of the market and ends at least 5 years at a date defined by the manufacturer**

9. Vulnerability Handling Requirements

2. Notified Body responsibilities

The notified body must verify that:

- vulnerability handling processes are documented
- remediation procedures and timelines are defined
- update distribution mechanisms are secure
- vulnerability management processes meet **CRA cybersecurity requirements**.

10. Documentation and Communication

The manufacturer must maintain **documentation demonstrating compliance**.

**1. Manufacturer responsibilities - **Documentation should include:

- cybersecurity risk assessments
- development and testing documentation
- security architecture descriptions
- vulnerability management procedures
- security update mechanisms.

The manufacturer must also provide **security-related information to users**, including vulnerability information and updates.

2. Notified Body responsibilities

- review the documentation supporting conformity assessment
- verify that documentation is **complete, accurate, and maintained**
- ensure that documentation enables monitoring of compliance.

11. Conformity Assessment and Surveillance

Module H includes **initial certification and continuous monitoring**.

1. Manufacturer responsibilities

- maintain the certified quality system
- implement corrective actions when required
- inform the notified body about significant changes to processes or products.

2. Notified Body responsibilities

- conduct **initial audits**
- perform **periodic surveillance audits***
- verify that the system continues to produce compliant products
- withdraw certification if requirements are no longer met.

*frequency to be detailed

11. Conformity Assessment and Surveillance

Compliance for the EU Market - CE Marking

Default products

- Self-assessment by the manufacturer
- EU Declaration of Conformity issued by the manufacturer
- CE marking

Important (Class I, II) and Critical products

- Conformity assessment by a Notified Body
- EU Declaration of Conformity issued by the manufacturer
- CE marking accompanied by the Notified Body identification number

12. Architecture of CRA Compliance under Module H

1 Regulatory requirements Cyber Resilience Act (CRA)

- Article 13 - Cybersecurity risk assessment
- Article 14 – Reporting obligations
- Annex I Part I - Product cybersecurity requirements
- Annex I Part II - Vulnerability handling requirements

2 Quality Assurance System ISO 9001

- organizational context and scope
- risk assessment and risk treatment
- operational processes
- documentation and monitoring.

Processes related to **products with digital elements and their supporting services**.

3 Product Security Processes

Security processes include:

- **secure development lifecycle**
- **management of technical vulnerabilities**
- These processes support the implementation of CRA cybersecurity requirements.

4 Product Lifecycle Coverage

The security processes must cover:

- design, development and production of the product
- vulnerability handling during the product support period
- security of remote services supporting the product.

5 Conformity Assessment (Module H)

A **Notified Body** evaluates the manufacturer’s quality system and verifies that the implemented processes ensure compliance with CRA cybersecurity requirements.

Download Eurosmart’s Guide on Module H implementation

Eurosmart’s Guide to Full Quality Assurance for CRA’s Conformity Assessment

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com

@Eurosmart_EU

@Eurosmart

Join Eurosmart – The Voice of the Digital Security Industry

https://www.eurosmart.com/how-to-join/

Eurosmart | Square de Meeûs 35| 1000 Brussels | Belgium