EUROSMART

The Voice of the Digital Security Industry

Implementing Module H under the Cyber Resilience Act:

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

Introduction

The Cyber Resilience Act (CRA) requires manufacturers of products with digital elements to demonstrate security by design and effective vulnerability handling across the entire lifecycle. While the CRA remains product-centric, focusing on the conformity of each product with the essential cybersecurity requirements, manufacturers can benefit from a system-level approach to streamline compliance.

This Eurosmart guide explains how to use **Module H - Full Quality Assurance** to meet those obligations through an auditable, process-centric approach.

The following represents our interpretation of how Module H could be applied in practice, based on our current understanding and experience with quality assurance frameworks. By leveraging existing quality systems (e.g., ISO 9001) and aligning them with the CRA's essential cybersecurity requirements (Annex I, Parts I & II), Module H enables Notified Bodies to audit the manufacturer's quality system and verify its implementation on representative products and without mandating exhaustive product-by-product testing.

Table of Contents

Disclaimer

Every effort has been made to ensure that the information in this document is accurate, clear, and relevant. However, Eurosmart, its members, and contributors cannot be held responsible for any errors, omissions, or outcomes resulting from its use.

Readers are encouraged to consider this guide as a supporting reference and remain solely responsible for evaluating its applicability to their own circumstances and for ensuring full compliance with all relevant European and national legislation.

1. What must be audited by the Notified Body

Under Module H, the Notified Body (NB)audits the manufacturer's quality system and tests its implementation on a set of representative products. The objective is to ensure that the manufacturer applies a comprehensive quality assurance system and that the resulting processes and products comply with the essential cybersecurity requirements of the CRA.

The NB may, where appropriate, conduct a combined audit that confirms compliance with both the CRA essential cybersecurity requirements and with an existing quality management standard such as ISO 9001, using a single audit framework.

Where the manufacturer already holds a valid ISO 9001 certificate, the Notified Body may rely on that certification and focus its audit primarily on the CRA essential cybersecurity requirements (Annex I Parts I and II).

The certificate of conformity issued by the Notified Body under the CRA covers all products manufactured under the audited processes, even if not all product types were directly sampled during the audit. An audit under Module H does not require all generic product types to be tested, provided the processes audited demonstrably cover those product categories. The Notified Body's role is to audit the quality system, not necessarily to test the implementation on each product.

The selection of representative products for sampling is at the discretion of the Notified Body, based on relevance, risk, and representativeness.

Would products be attached to ***remote data processing*** the absence of which would prevent such products with digital elements from performing one of their functions, the audit shall cover the corresponding ***remote data processing*** solution(s)**.**

The Module H imposes ongoing obligations, not just one-off testing. The manufacturer shall keep the Notified Body that has approved the quality system informed of any intended change to the quality system.

2. When Full Quality Assurance can be used?

A conformity assessment based on full quality assurance (based on module H) can be used for any product with digital elements[1], and in particular, can be used for important products of Class I and class II as well as for critical products.

For critical products undergoing a European cybersecurity certification, Module H can be used to demonstrate their conformity to the Essential Cybersecurity Requirements of the CRA.

[1] Regulation (EU) 2024/2847 - Article 3(1) provides: "product with digital elements' means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately".

3. Overview of manufacturers' obligations

The manufacturer shall operate a quality system for:

- Design, development, testing and production
- Vulnerability handling

The manufacturer shall maintain its effectiveness over the support period, and the maintenance might be subject to surveillance by the Notified Body

In essence, the quality system must cover the full lifecycle of the product, including how vulnerabilities are handled. The quality system must ensure:

- compliance of the products with essential cybersecurity requirements (Annex I Part I)
- compliance of the manufacturer's vulnerability handling processes with Part II of Annex I and article 14
- compliance with customer and regulatory requirements, for example by using standards such as ISO 9001

The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market or for the support period, whichever is longer, keep at the disposal of the national authorities the documentation related to audits and surveillance.

4. Full Quality Assurance Assessment: Key Steps

1. The manufacturer must submit an application to a Notified Body for assessment of its quality system for the concerned products. The application must include:
    a) name/address of manufacturer (and authorised representative if applicable)
    b) the technical documentation for one model of each product CRA category
    c) documentation concerning the quality system
    d) a declaration that the same application was not lodged with another Notified Body
2. During the audit, the manufacturer must make available to the NB both the technical documentation and the quality system documentation. The quality system must explicitly include controls, procedures, checks, traceability, etc.
3. After the audit, the manufacturer must affix the CE marking[2] and draw up the EU declaration of conformity, stating that Module H was used and that both products cybersecurity and vulnerability handling processes comply with CRA requirements. The declaration of conformity is under the manufacturer's sole responsibility
4. After approval, periodic surveillance or auditing is required. The Notified Body shall ensure that the quality system is properly maintained. The manufacturer must allow the Notified Body access to relevant documentation to verify compliance over time.

[2] The manufacturer shall ensure that the CE marking is clearly visible, legible and indelible on the product or, where not feasible (for example small items or purely digital products), on the packaging or documentation. If the product is very small (e.g., a tiny board or embedded module) making the CE mark physically challenging to fit, the manufacturer should document the reasoning and ensure that packaging or accompanying documentation carries the marking.
The CE marking shall be followed by the identification number of the notified body

5. Compliance with the CRA Essential Cybersecurity Requirements

This chapter establishes the link between the essential cybersecurity requirements of the CRA and the elements that the Notified Body must examine during its audit.

The quality system to be audited must cover both quality and cybersecurity aspects. To this end, Documented information must be made available to the Notified Body

This chapter describes the elements that must be included in Documented information, with reference to the provisions of the CRA.

5.1 Risk Analysis

(**Annex I + Annex VII + Annex VIII**)

LEGAL REFERENCE	REQUIRED ACTION / DOCUMENTATION
ANNEX I (PART I INTRO & POINT 1)	**Perform a cybersecurity risk analysis:** identify and evaluate risks the product presents, considering **intended use, misuse, and connectivity.**
ANNEX VII § 3	**Document the analysis and assessment of the risks** in the **technical documentation**. It must be "adequate" and allow assessment of conformity.
ANNEX I (PART I POINT 2)	Use the results to design protections proportionate to those risks (secure design, default configuration, resilience, data protection).
ANNEX VIII PTAR IV § 2–3	Integrate the risk analysis procedure into the **quality system**, ensuring risks are re-evaluated during design, development, and support.
ANNEX VIII PTAR IV § 3(1)(B)	Include the **risk analysis report** as part of the technical documentation **for one model of each product category** submitted to the Notified Body.
ANNEX VIII PTAR IV § 4 & ART. 10	**Maintain and update the risk analysis throughout the supporting period** and **when vulnerabilities or design changes arise.**

Expected content of risk analysis file

1. Product description and intended purpose.
2. Identified cybersecurity threats and potential attack vectors.
3. Likelihood and impact estimation.
4. Resulting overall risk level.
5. Mapping of mitigation measures to Annex I requirements.
6. Record of residual risks and justification.
7. Review/update procedure over lifecycle.

5.2 Quality System

(**Annex VIII Part IV § 2–3**)

LEGAL REFERENCE	EVIDENCE / NOTES
ANNEX VIII PT IV § 2	Implement and document **a quality system** covering - Design, development, testing and production - Vulnerability handling In essence, the quality assurance system must cover the full lifecycle of the product, including how vulnerabilities are handled
ANNEX VIII PT IV § 3(2)(a)	Include a description of the **quality objectives**, organisational structure, and management responsibilities and powers relating to design, development, product quality, and vulnerability handling.
ANNEX VIII PT IV § 3(2)(b)	**Compliance with Essential cybersecurity requirements**[3] Include the **technical design and development specifications**, including possibly the *Harmonised Standards* or *Technical Specifications* [4]applied to facilitate compliance with the Annex I Part I ("essential requirements); Where neither *Harmonised Standards* nor *Technical Specifications* are not applied or partially applied, then mapping describing the **means** used to ensure conformity with the essential cybersecurity requirements
	Compliance with Vulnerability Handling

[3] *In B2B environments, the supplier may have limited control over certain essential requirements, notably:*

(l) Providing mechanisms to record and monitor relevant internal activity (e.g. access or data modification) with an opt-out mechanism for users;

(m) Providing users with secure and easy means to permanently erase data and settings, and to transfer such data securely where applicable.

These should be addressed contractually or through interface documentation to ensure compliance where the supplier's control is partial.

[4] *The application of harmonised standards and technical specifications under the Cyber Resilience Act (CRA) and other relevant EU legislation is voluntary. Their use provides a presumption of conformity with the corresponding essential requirements.*

When harmonised standards or technical specifications are not applied, the organisation shall demonstrate conformity by other appropriate means, such as the use of an internal cybersecurity framework, independent testing and validation reports, technical justifications, or equivalent documented evidence.

Within the framework of the Quality Management System (QMS) compliant with ISO 9001, the selection, application, and justification for the use of standards, harmonised standards or other means shall be documented and reviewed to ensure continued compliance with applicable regulatory and quality requirements.

ANNEX VIII PT IV § 3(2)(c)	Include the **procedural specifications**, including standards, for ensuring compliance with the **Annex I Part II** (vulnerability handling) requirements. - explain alternative means where harmonised standards, technical specifications are not applied or partially applied.
ANNEX VIII PT IV § 3(2)(d)	Describe **design and development control** and **verification techniques**, processes and systematic actions used during design and development of the products.
ANNEX VIII PT IV § 3(2)(e)	Describe **production, quality-control and quality-assurance techniques, processes and systematic actions** used during manufacture.
ANNEX VIII PT IV § 3(2)(f)	List the **examinations and tests** performed before, during and after production, and their **frequency**.
ANNEX VIII PT IV § 3(2)(g)	Specify the **quality records** maintained (inspection reports, test data, calibration data, personnel qualification reports).
ANNEX VIII PT IV § 3(2)(h)	Define the **means of monitoring** the achievement of the required design and product quality and of the **effective operation of the quality system**.
ANNEX VIII PT IV § 3(3–5)	Undergo notified-N Body assessment, implement corrective actions if required, and obtain approval of the quality system.

5.3 Vulnerability Handling

Within Module H, vulnerability handling must be included as a core process, structured like design or production control.

the standard Information technology - Security techniques - Vulnerability handling

QUALITY-SYSTEM ELEMENT (ANNEX VIII PT IV § 3(2))	HOW VULNERABILITY HANDLING FITS?
(a) QUALITY OBJECTIVES, ORGANISATION, RESPONSIBILITIES	Define a cybersecurity manager or team responsible for vulnerability coordination; specify authority to trigger security updates and external notifications.
(b) TECHNICAL DESIGN/ DEVELOPMENT SPECIFICATIONS	Include security-update mechanisms, patch distribution channels, and secure coding standards that enable remediation, whenever possible.
(c) PROCEDURAL SPECIFICATIONS	Contain the vulnerability-handling procedures (identification, assessment, prioritization, mitigation, disclosure).

(d) DESIGN-CONTROL AND VERIFICATION TECHNIQUES	Describe how vulnerabilities remediation is verified, validated, and functional regression-tested before patch release.
(e) PRODUCTION/QA TECHNIQUES	Include checks ensuring updates are correctly built, signed, and made available to stakeholders.
(f) EXAMINATIONS AND TESTS	Define penetration tests, code security reviews, and other secure testing for patches and security updates.
(g) QUALITY RECORDS	Maintain logs of vulnerabilities, CVE IDs, patch tests, disclosure communications.
(h) MONITORING OF QUALITY-SYSTEM PERFORMANCE	Include internal audits, metrics (e.g. mean time to fix), management review of vulnerability handling effectiveness.

5.4 Application

Annex VIII Pt IV § 3(1)(a–d)	The manufacturer must submit an application to a Notified Body for assessment of its quality system for the concerned products The application must include: a) name/address of manufacturer (and authorised representative if applicable) b) the technical documentation for one model of each product category c) documentation concerning the quality system d) a declaration that the same application was not lodged with another Notified Body

5.5 Declaration and Marking

(**Annex VIII Part IV § 5 + Annex V + Art. 33**)

LEGAL REFERENCE	EVIDENCE / NOTES
§ 5(1) + ANNEX V	**Draw up EU Declaration of Conformity stating Module H and compliance with Annex I requirements.** The declaration is under the manufacturer's sole responsibility
§ 5(2) + ART. 33	**Affix CE marking.**
ART. 31 (2)	Keep Declaration and technical documentation (including risk analysis) for 10 years after placing on market.

6. Module H and assessment by the NB

6.1 Assessment

The Notified Body follows a structured procedure that includes the following key steps:

(**Annex VIII Part IV § 3 (3–5)**)

LEGAL REFERENCE	EVIDENCE / NOTES
§ 3(3) **+BLUEGUIDE**	Undergo notified-bodyNB evaluation of **quality system and supporting risk analysis.** **1. Definition of the scope of audit** - The scope (generic types, subtypes, and articles) is agreed between the manufacturer and the Notified Body.
§ 2–3 **+BLUEGUIDE**	**2. Review of quality management documentation** - The Notified Body reviews the Documented information both before and during the audit

6.2 Documented information

Under **Annex VIII Part IV § 2–3**, the Documented information provides the structured documentation of the quality system that the Notified Body audits.

It demonstrates that all processes - from design to vulnerability handling - operate under control and meet the CRA essential requirements of **Annex I Parts I and II.**

The documented information should generally align with ISO 9001 and ISO 17025, covering:

- Design and development phases,
- Relevant production steps (incoming goods inspection, traceability of raw materials, in-process inspections, etc.),
- Testing requirements for final inspection and verification.

CRA REFERENCE (ANNEX VIII PART IV)	CRA REQUIREMENT	TYPICAL CONTENT IN THE DOCUMENTED INFORMATION	PURPOSE
§ 2(a)–(b)	Operate a quality system covering **design, development, production, final inspection, testing, and vulnerability handling**	Documented information describing organisational structure, process flow, and interfaces between design, manufacturing, testing, and security management	Establishes the scope of the full-quality-assurance system

§ 3(2)(a)	**Quality objectives, organisation, and responsibilities**	Quality policy, management roles, internal communication, competence matrix.	Shows management control and accountability for product conformity
§ 3(2)(b)	**Technical design and development specifications** ensuring conformity with **Annex I Part I**	Design-control procedures, product-spec documentation, design verification and validation, configuration management	Demonstrates that design activities ensure cybersecurity and safety by design
§ 3(2)(c)	Procedural specifications covering vulnerability handling (Annex I Part II)	Reference to Documented information or integrated section describing identification, assessment, disclosure, and mitigation of vulnerabilities	Links general quality control with CRA-specific vulnerability obligations
§ 3(2)(d)	**Design-control and verification techniques**	Design review gates, verification protocols, independent validation, change-control procedures	Ensures design outputs meet input requirements and traceability is maintained
§ 3(2)(e)	**Production, quality-control, and quality-assurance techniques**	Incoming goods inspection, traceability of materials, in-process controls, calibration and test-equipment management	Ensures consistent manufacturing quality
§ 3(2)(f)	Examinations and tests before, during, and after production	Test plans, sampling procedures (e.g. ISO 2859-1), acceptance criteria, environmental and functional testing	Confirms that every batch or article meets specification
§ 3(2)(g)	**Quality records**	Templates and logs for inspection results, calibration certificates, training records, incident reports	Provides traceability and evidence of conformity
§ 3(2)(h)	**Monitoring of quality-system performance**	Internal audit plan, management review minutes, KPI dashboards, corrective-/preventive-action system	Ensures continuous improvement and ongoing compliance
§ 3(3)–(5)	**Assessment and approval by the Notified Body**	Procedures for NB interaction, corrective-action tracking, management of audit findings	Facilitates surveillance and re-approval under Module H

If products depend on remote data processing (e.g. cloud components) essential to their operation, Documented information must include DevOps and lifecycle management processes for these remote elements.

The Documented information should also address design, development, production, testing, and maintenance of cybersecurity controls and correspond to the cybersecurity-specific parts of Annex VIII Part IV § 3(2) particularly:

CRA REFERENCE	CRA REQUIREMENT	TYPICAL CONTENT IN THE DOCUMENTED INFORMATION	PURPOSE / COMMENT
§ 2(a)–(b) + Annex I Part I intro	Operate a quality system covering **design, development, production, final inspection, testing, and vulnerability handling** from a cybersecurity perspective	Cybersecurity governance model; secure-by-design principles; mapping between product lifecycle and CRA essential requirements	Integrates cybersecurity assurance within the overall quality system defined in the Documented information
§ 3(2)(a) + Annex I Part I (1)	**Quality objectives, organisation, responsibilities** relating to cybersecurity	Roles and responsibilities of the Cybersecurity Manager, Cybersecurity Architect; escalation and decision-making processes	Demonstrates management control and accountability for cybersecurity conformity
§ 3(2)(b) + Annex I Part I (2)(a–k)	**Technical design and development specifications** ensuring compliance with essential cybersecurity requirements	Threat-modelling methodology, secure architecture design, coding standards, crypto policy, default-configuration rules, and security-test plans	Provides traceable evidence that the product meets Annex I Part I technical requirements
§ 3(2)(c) + Annex I Part II (1–3)	**Procedural specifications for vulnerability handling**	Product Security Incident Response Team (PSIRT); Vulnerability management policy, CVE tracking, risk scoring (CVSS), coordinated-disclosure process, patch-management or mitigation plan workflow, communication with ENISA/CSIRTs	Ensures fulfilment of Annex I Part II (vulnerability handling and reporting) obligations
§ 3(2)(d)	**Design-control and verification techniques**	Security design-review checkpoints, independent code review, penetration-testing procedure, regression-test validation before patch release	Confirms that security controls are verified and validated throughout the lifecycle

§ 3(2)(e)	**Production and QA techniques from a cybersecurity standpoint**	Secure-build environment policy, code-signing procedure, supply-chain-integrity checks, firmware-validation tests	Ensures that production and release processes maintain cybersecurity integrity
§ 3(2)(f)	**Examinations and tests**	Security-test plans, fuzzing and penetration-test protocols, vulnerability-scanning frequency, acceptance criteria	Demonstrates systematic testing of cybersecurity properties before and after release
§ 3(2)(g)	**Quality records**	Vulnerability logs, security-incident registers, penetration-test results, patch validation reports, disclosure communications	Provides traceability and evidence of cybersecurity assurance activities
§ 3(2)(h)	**Monitoring of quality-system performance**	Security metrics (mean time to fix, patch coverage, vulnerability recurrence rate), internal audits, management review reports	Ensures continual improvement of cybersecurity performance
§ 3(3)–(5)	**Assessment and approval by the Notified Body**	Interface procedure with NB: documentation delivery, response to audit findings, corrective actions on security-related non-conformities	Allows NB to verify that cybersecurity and vulnerability-handling processes meet CRA requirements
Annex I Part I (2)(l–m)	**User-facing security requirements** (monitoring and secure erasure)	Design notes on audit-log mechanisms, data-erasure functions, transfer-security features	Addresses essential requirements often partially under supplier or integrator control (esp. B2B contexts)

6.3 Audit team composition

Typically, two auditors participate, ensuring impartiality and covering both technical and organisational/legal aspects.

6.4 Checks performed during the audit

a. Verification of risk assessment processes according to CRA Annex I Part I(1).
b. Review of design phase documentation (security architecture, design specs, etc.) for compliance with Annex I Part I(2)(c-k).
c. Review of **security management and testing plans** for Annex I Part I(2)(a).
d. Assessment of default configuration and security guidance for compliance with Annex I Part I(2)(b).

6.5 Additional production-related checks

e. Incoming goods inspection, traceability of materials and intermediates.
f. In-process inspection procedures.
g. Sampling practices (with possible justified deviations from ISO 2859-1).
    i. Final product testing capabilities at the test site.
    ii. Handling of non-conformities: documentation and treatment of non-conforming lots or articles.

§ 3(4–5)	Address findings, implement corrective actions, obtain formal approval of the quality system.

7. Surveillance and Maintenance

After approval, periodic surveillance or auditing is required

(**Annex VIII Part IV § 4**)

LEGAL REFERENCE	**EVIDENCE / NOTES**
+BLUEGUIDE	**Reporting and follow-up** ○ At the end of the audit, the Notified Body provides an abridged audit report (oral or written summary of findings and requirements). ○ A comprehensive audit report is drawn up after completion, in accordance with 2013/29/EU Annex II Module H § 4.3, detailing actions, observations, and requirements. ○ Periodic surveillance audits are conducted (typically every two years), adjusted based on performance, previous findings, and market surveillance outcomes. **Certification and registration** ○ After all requirements are met, the Notified Body issues a certificate of conformity, defining: ▪ The validity period (linked to surveillance frequency), ▪ The **categories/generic types/articles** covered. ○ The registration procedure may include the following: ▪ The manufacturer submits a type test report; ▪ The Notified Body performs an Essential Requirements (ESR) assessment; ▪ The NB issues the assessment report, registration number, and related documentation.
§ 4(1–2)	Ongoing audits (usually annual) verifying maintenance of the approved system and updated risk analysis.

§ 4(3–4)	Manufacturer to notify Notified Body of any intended changes affecting conformity; implement their decisions on re-assessment.

(**Annex I Part II + Art. 10–11**)

LEGAL REFERENCE	EVIDENCE / NOTES
ANNEX I PART II	Operate vulnerability handling processes (discovery, coordinated disclosure, patching, notification).
ART. 11	Notify significant exploited vulnerabilities or severeincidents to the relevant CSIRT / ENISA.
ANNEX VIII PT IV § 2	Maintain the QA system's effectiveness during the entire support period.

8. Conclusion

Module H offers manufacturers a structured and efficient pathway to demonstrate conformity with the Cyber Resilience Act while embedding cybersecurity assurance into their existing quality systems. By shifting the focus from product-by-product testing to a comprehensive, lifecycle-oriented assessment, this approach strengthens both security and operational efficiency.

Through a well-documented quality system, robust risk-analysis procedures, and effective vulnerability-handling processes, manufacturers can provide Notified Bodies with clear evidence of compliance with the CRA's essential cybersecurity requirements. The integration of secure-by-design principles into design, development, production, and maintenance not only supports regulatory conformity but also enhances trust in digital products placed on the EU market.

As the voice of the European digital security industry, Eurosmart notes that many ICT providers already operate mature Quality Management Systems and have experience with cybersecurity certification schemes such as EUCC. For these actors, Module H represents the most natural and efficient pathway to demonstrate CRA conformity, particularly for products already certified under EUCC. Leveraging existing processes and audit frameworks allows them to streamline compliance efforts while maintaining a high level of assurance.

Successful implementation of Module H relies on transparency, traceability, and continuous improvement. Ongoing surveillance by the Notified Body, combined with the manufacturer's commitment to maintaining and updating their processes throughout the product's support period, ensures that cybersecurity remains an active and sustained responsibility.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com