EUROSMART
The Voice of the Digital Security Industry

ISO 9001 and Module H:

A scalable approach to CRA conformity assessment

September 2026

About Eurosmart

Eurosmart is a European not for profit organisation dedicated to advancing the digital security industry through innovation, standardisation and certification, and advocacy. With a rich history spanning decades, Eurosmart serves as a trusted voice in the field, representing a diverse range of stakeholders. Its members include manufacturers of secure elements, semiconductors, smart cards, systems-on-chip, high-security hardware and terminals; providers of biometric technologies, secure software and cloud services; system integrators; application developers; and issuers. The membership also encompasses security evaluation laboratories, consulting firms, research organisations and industry associations.

Committed to fostering a secure and trustworthy digital environment, Eurosmart engages in proactive initiatives to promote the adoption of robust security solutions and standards. By leveraging its expertise and extensive network, Eurosmart plays a pivotal role in shaping the future of cybersecurity and digital transformation across Europe and beyond.

Executive Summary

The Cyber Resilience Act provides Full Quality Assurance, based on Module H of the New Legislative Framework, as a conformity assessment route for **Important and Critical Products with Digital Elements (PwDEs)**. This approach is particularly relevant for manufacturers managing large product portfolios, product families and legacy products.

ISO 9001 provides a natural and scalable management-system foundation for CRA Module H. CRA-specific cybersecurity processes can be integrated into an existing Quality Assurance System (QAS), without requiring a separate Information Security Management System (ISMS). **ISO 9001 provides the foundation upon which CRA-specific requirements and product-specific evidence can be integrated and assessed under Module H:** Notified Bodies assess and supervise the extended QAS, its CRA-specific cybersecurity processes and the relevant product-specific evidence against the applicable CRA requirements.

By combining **established quality assurance practices, cybersecurity expertise and product-specific evidence**, Module H provides a proportionate and scalable approach to conformity assessment. It can reduce unnecessary duplication, make efficient use of Notified bodies' capacity and facilitate the timely implementation of the CRA while maintaining the required level of cybersecurity assurance.

Table of Contents

1. Why the CRA includes a Module H-based conformity assessment

1.1. The regulatory framework

The Cyber Resilience Act (CRA) establishes several conformity assessment procedures in Annex VIII. For Important and Critical Products with Digital Elements (PwDE), manufacturers may demonstrate conformity through Conformity based on Full Quality Assurance (based on Module H – Article 32 and Annex VIII - Part IV[1]). Unlike the original New Legislative Framework modules, established in Decision No 768/2008/EC, the CRA adapts these procedures to cybersecurity by explicitly requiring the assessment of the manufacturer's vulnerability handling processes in addition to product conformity.

Under Module H, the manufacturer operates a **full quality assurance system covering design, manufacturing, final inspection, and testing during it whole lifecycle**, while a **Notified Body** assesses and continuously supervises that system.

The rationale for this approach is set out in Recital 91 of the CRA. Recognising both the importance of cybersecurity during the design and development of products and the need to avoid unnecessary administrative burden, the legislator identified conformity assessment procedures based on Modules B+C and Module H as the most appropriate mechanisms for demonstrating conformity of Important PwDEs. For Critical PwDEs, Article 32 similarly provides Module H as one of the applicable conformity assessment routes. Module H therefore constitutes a common regulatory pathway available under the CRA for both Important and Critical PwDEs, subject to the applicable conditions of Article 32. Thus, with the "Module compliance approach" manufacturers can demonstrate conformity through an approved quality assurance system rather than repeated product-based assessments.

1.2. Cybersecurity requires process assurance

Cybersecurity depends on the manufacturer's ability to establish, implement and maintain controlled engineering and manufacturing processes throughout the product lifecycle. These processes cover secure design and development, software maintenance, vulnerability handling, security updates and other lifecycle activities that continue long after a product has been placed on the market.

For this reason, the CRA and its Essential Security Requirements (ESRs) with a module H approach extends the traditional concept of Full Quality Assurance beyond product quality alone. In addition to assessing the quality of the product, it requires an assessment of the processes and evidence that support cybersecurity throughout the supported lifetime of the product to establish a compliance (formalized with a CE marking).

The Module H approach is particularly relevant for products requiring a higher level of assurance, including Important Products with Digital Elements, particularly Class II, Critical PwDEs where Module H is an applicable conformity assessment route, and products already subject to cybersecurity certification.

[1] The CRA does not invent Module H. It reuses the conformity assessment modules established in Decision No 768/2008/EC, adapting them to cybersecurity. This is why Article 32 refers to procedures "based on Module H", while Annex VIII contains the CRA-specific version.

Manufacturers of such products usually rely on mature and controlled development, production and vulnerability handling processes. At the same time, individual products may already be subject to extensive security evaluation or certification. Module H allows these common organisational processes to be assessed and supervised at manufacturer level, while product-specific evidence remains necessary to demonstrate compliance with the applicable cybersecurity requirements.

2. Building on existing quality assurance systems

For many manufacturers, Module H is a practical conformity assessment route because it can build on a mature Quality Assurance System (QAS), often certified to ISO 9001, covering design, development, manufacturing, supplier management and change control.

Rather than creating a separate system for CRA compliance, manufacturers can integrate the cybersecurity practices required by CRA Annex I - product cybersecurity requirements and vulnerability handling - into this existing engineering and quality framework.

2.1. ISO 9001 provides the natural foundation for Module H

2.1.1. Regulatory recognition of ISO 9001

The Full Quality Assurance procedure established by the CRA is based on the assessment of the manufacturer's assurance system. While the CRA introduces cybersecurity-specific obligations, the underlying principles remain those of a controlled engineering organisation capable of consistently designing, developing and maintaining compliant products.

Several authoritative sources recognise ISO 9001 as a relevant foundation for CRA Module H conformity assessment:

- **This is reflected in Decision No 768/2008/EC**, which associates Module H with ISO 9001 in its table of conformity assessment procedures.[2]
- **The CRA FAQ (§6.3)**[3] similarly explains that the full quality system may be based on international standards, including the ISO 9000 series, adapted to the specificities of the CRA.
- **Blue Guide 2022 §5.1.6** - Modules based on quality assurance*: "Compliance of the manufacturer with standards EN ISO 9000, EN ISO 9001, gives a presumption of*

[2] Decision No 768/2008/EC of the European Parliament and of the Council establishes the common framework for the marketing of products under the **New Legislative Framework (NLF)** by defining the standard conformity assessment modules (Modules A to H) used as the basis for sector-specific Union harmonization legislation. The Cyber Resilience Act follows this approach by establishing, in Annex VIII, conformity assessment procedures **based on** Modules B, C and H of Decision No 768/2008/EC, while adapting them to the specific cybersecurity objectives of the Regulation.
The **Table of Conformity Assessment Procedures in Community Legislation** annexed identifies **EN ISO 9001** as the reference Quality Assurance System standard associated with Module H. The CRA further extends Module H by requiring that the manufacturer's vulnerability handling processes comply with Annex I, Part II of the Regulation

[3] C(2026) 5252 - Annex - Commission guidance on the application of the Cyber Resilience Act (CRA)

conformity with the corresponding quality assurance modules as regards the legislative provisions covered by these standards."

2.1.2. Extending ISO 9001 to cybersecurity

The CRA Module H procedure is explicitly structured around a Quality Assurance System. It does not require manufacturers to establish a separate Information Security Management System (ISMS) or another parallel cybersecurity management system.

For manufacturers already operating an ISO 9001-certified QAS, the natural approach is therefore to integrate the CRA-specific cybersecurity activities into that existing quality framework. These activities may be supported by specialised cybersecurity standards and methodologies, but such standards complement the QAS; they do not replace it or constitute an additional management-system prerequisite for Module H.

Cybersecurity processes can draw upon various standards and methodologies, depending on the industry sector, the country of deployment, or the technologies involved. It is essential to maintain the ability to adapt effectively to specific use cases, as relying on a single standard would impoverish current practices.

Taking risk management methods as an example, the best approach is to identify the most suitable options from among the most widely adopted practices: EBIOS, BSI Standard 200-3 / IT-Grundschutz, ETSI TS 102-165 (TVRA), TARA (automotive and embedded products), STRIDE (software architecture security), FAIR (cyber risk quantification) ... Related Cybersecurity processes can then refer to mature methodologies but be refined for specific use cases.

Similarly, there is no single universal standard for Design, Integration, Verification & Validation (IV&V) in the context of product cybersecurity. Instead, organisations generally rely on a set of standards and methodologies that define how cybersecurity requirements are specified, verified, validated, tested, and certified throughout the product lifecycle. Cyber processes may reference various standards and methodologies: ISO/SAE 21434, IEC 62443-4-1: Secure product development lifecycle, IEC 62443-4-2: Technical security requirements for products, IEC 62443-3-2: Risk assessment and system security, Common Criteria (ISO/IEC 15408) ... and be refined to best meet specific needs. Cybersecurity processes may also recommend LLM scanning, SAST, DAST, SCA, fuzzing, vulnerability assessment, and so on. They may also address the verification phase and outline penetration testing and red teaming activities.

Finally, standards and methodologies define how vulnerabilities, weaknesses, and security flaws should be corrected, mitigated, verified, and tracked to closure. Examples include NIST SP 800-40, IEC 62443, FIRST PSIRT, IEC 62443-4-1, ISO/SAE 21434, OWASP SAMM, Common Criteria (ISO/IEC 15408 Renewal/Patch Management) ...

There are numerous ways to implement the essential requirements of the CRA, and the variety of available methods and standards allows for this implementation to be closely tailored to specific cases. The practical implementation of these additional processes, and their integration within an existing Quality Assurance System, is described in the *Eurosmart Guide to Full Quality Assurance for CRA Conformity Assessment*[4].

[4] See *Eurosmart, Guide to Full Quality Assurance for CRA Conformity Assessment*, which provides practical guidance on implementing the cybersecurity processes required under Module H and integrating them into an existing Quality Assurance System.

It is not difficult to assess whether these additional processes cover the essential requirements, because the objectives are identical. Furthermore, it is easy for the manufacturer to provide a mapping of this coverage.

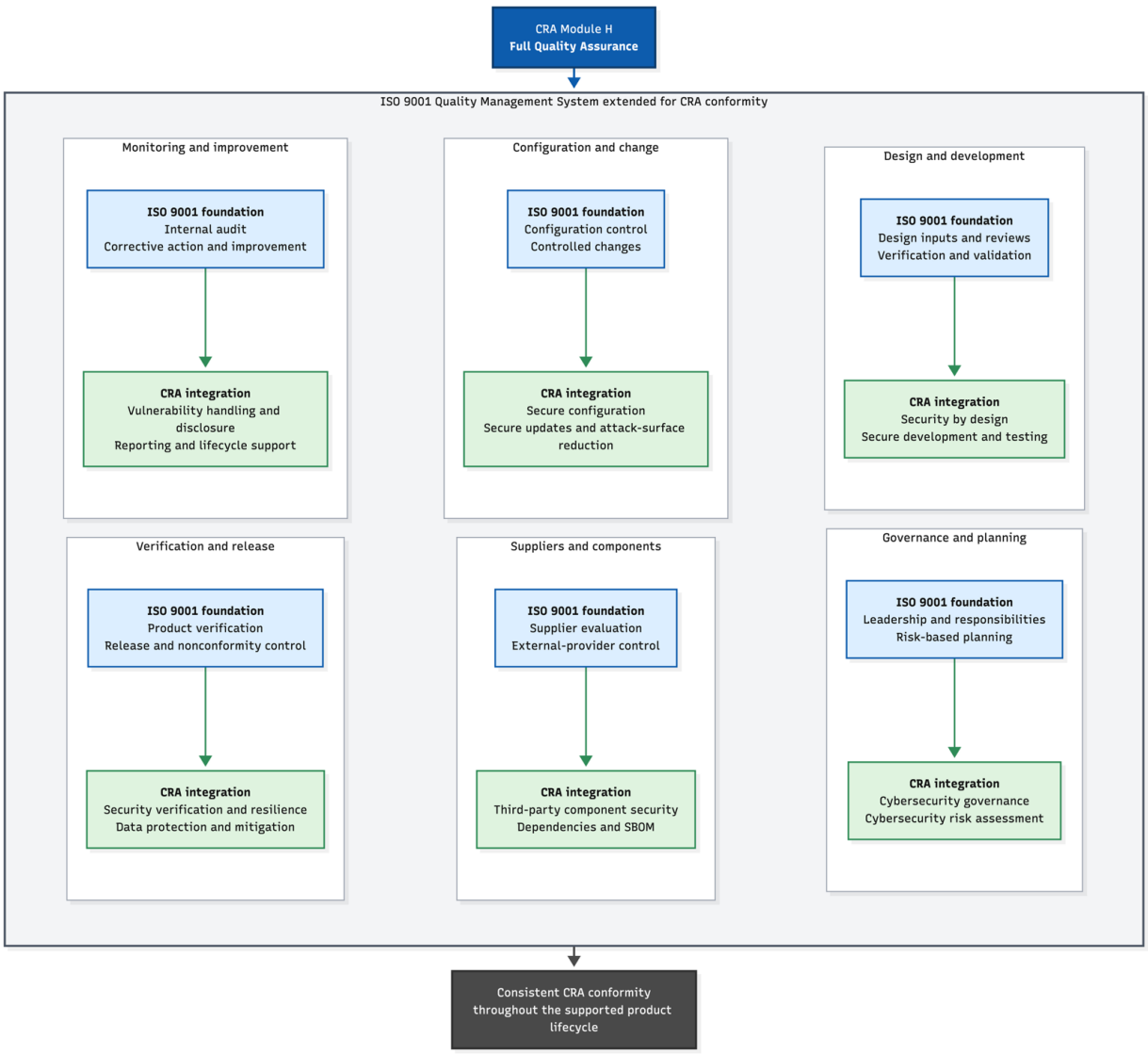
2.1.3. Process-oriented assurance for product families

Many manufacturers develop multiple product families that share common engineering practices, secure development processes, quality assurance activities and vulnerability handling procedures. Assessing these engineering capabilities separately for every product would lead to unnecessary duplication without necessarily improving the effectiveness of the conformity assessment.

This scalability is particularly important in the context of the CRA. Manufacturers may have extensive portfolios comprising multiple product families, variants and legacy products that will remain on the Union market when the CRA becomes applicable. Applying conformity assessment on a purely product-by-product basis would create significant duplication of assessment activities and could generate capacity bottlenecks for both manufacturers and Notified Bodies.

Module H provides a means to address this challenge by assessing common and repeatable organisational processes at manufacturer level, while maintaining the product-specific evidence necessary to demonstrate conformity of the products concerned.

Fig. 1 - Integration of CRA Cybersecurity Processes into an ISO 9001 Quality Assurance System



2.2. Cybersecurity assurance relies on controlled processes

This relationship has long been recognised by established cybersecurity assurance frameworks. Common Criteria (ISO/IEC 15408), for example, does not rely exclusively on the technical evaluation of a product. It also requires evidence that the Target of Evaluation has been developed under controlled processes.

3. A proportionate and scalable conformity assessment approach

3.1. Combining system assessment and product evidence

Under Module H, the engineering and manufacturing processes established within the manufacturer's QAS are **assessed once as part of the conformity assessment** and compliance for **each PwDEs' family** with applicable essential cybersecurity requirements is evaluated by sampling **evidence** for activities described and **performed** as per QAS (like technical documentation, cybersecurity risk assessments and product-specific).

This combination of management system assessment and product-specific evidence reflects the complementary nature of Module H.

- The QAS demonstrates that the engineering processes required to achieve and maintain cybersecurity are implemented consistently across the organisation throughout the product lifecycle.
- The technical documentation demonstrates that each PwDEs complies with the applicable essential cybersecurity requirements of Annex I and is supported by an appropriate cybersecurity risk assessment.

This approach is particularly relevant for manufacturers of **Important and Critical PwDEs** managing extensive product portfolios, product families, legacy products, or products that evolve through regular software releases. By assessing common processes once and combining this with appropriate product-specific evidence, Module H can reduce unnecessary duplication while preserving the level of assurance required by the CRA.

3.2. Audit competence and scalability

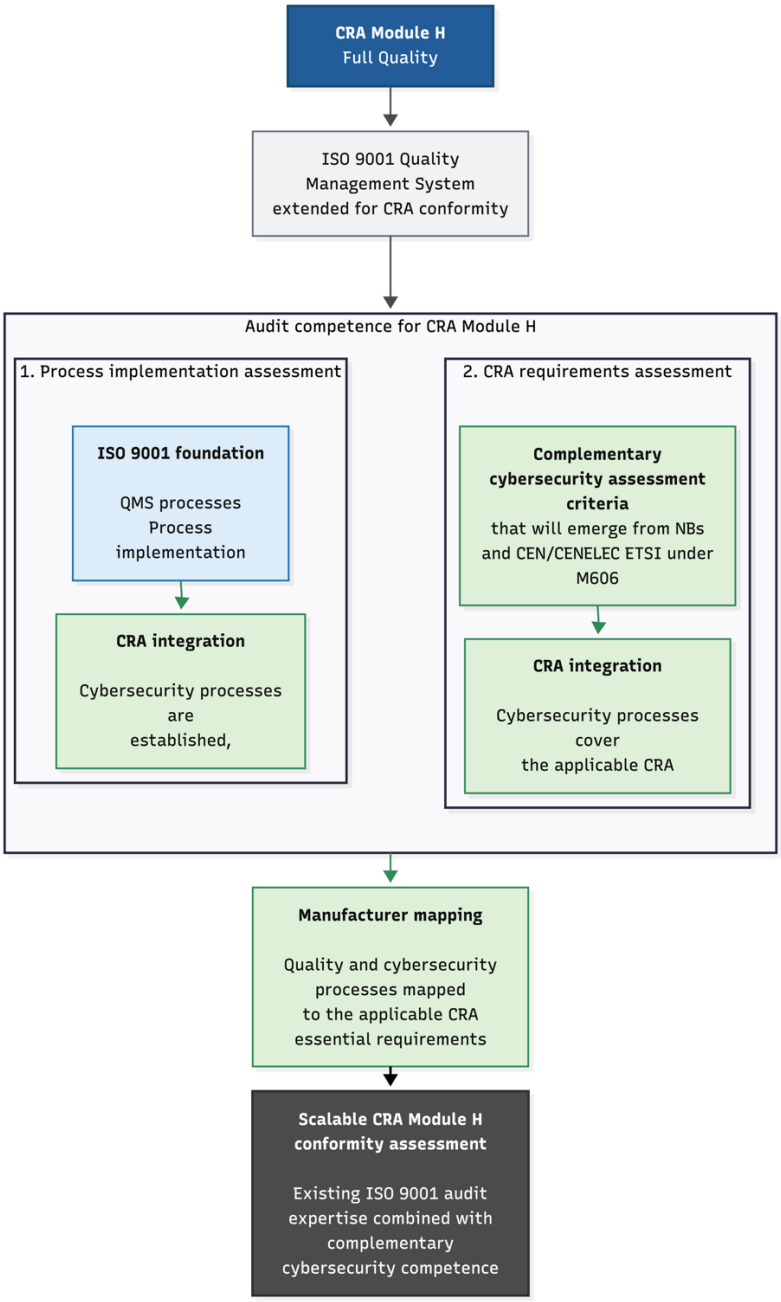
One of the strengths of the Module H approach is that it builds upon the well-established quality assurance auditing framework already used throughout European industry. ISO 9001 is the most widely implemented management system standard and is supported by a large community of qualified auditors across the European Union. This provides a strong foundation for the consistent and scalable assessment of manufacturers' quality assurance systems under Module H.

In the context of the CRA, Module H assessments extend conventional quality assurance audits by verifying that the manufacturer's cybersecurity processes are effectively integrated into the quality assurance system and consistently applied throughout the product lifecycle. This aspect of the assessment naturally builds upon established ISO 9001 auditing practices, while focusing on the additional ESRs required by the CRA.

The assessment also requires verification that these cybersecurity processes satisfy the essential cybersecurity requirements of the CRA. This requires complementary cybersecurity competence, particularly in secure development lifecycle processes and cybersecurity engineering. Relevant expertise may include standards such as IEC 62443-4-1, ISO/IEC 27034

and, where appropriate, ISO/IEC 27001. **These competencies complement rather than replace ISO 9001 quality assurance expertise.**

Fig. 2 - Leveraging ISO 9001 Audit Expertise for Scalable CRA Module H Conformity Assessment



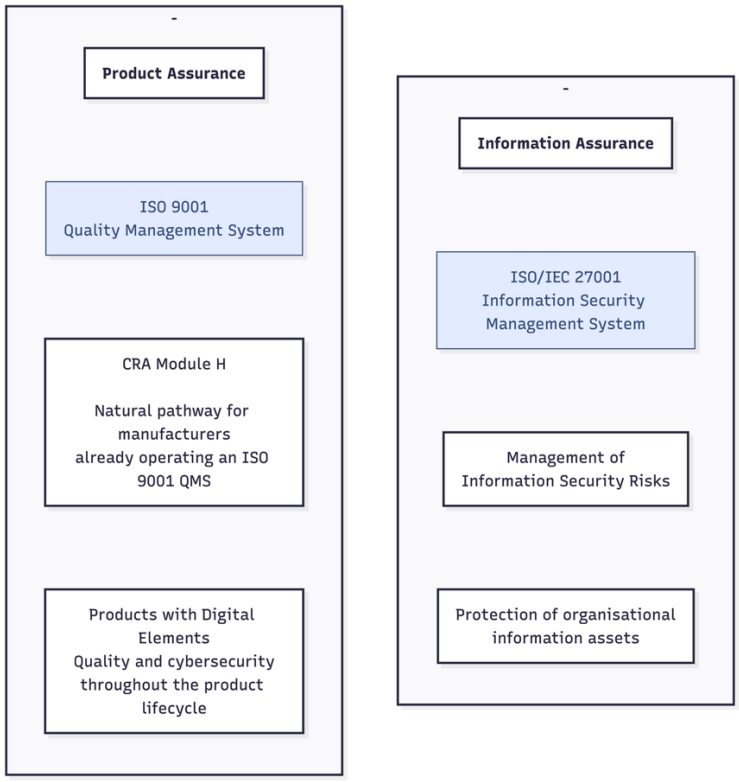
In practice, manufacturers can facilitate the assessment by providing documented mappings between their quality and cybersecurity processes and the applicable CRA essential requirements. This enables notified bodies to verify conformity in a structured and repeatable manner while avoiding unnecessary duplication of assessment activities. Consequently, Module H provides a conformity assessment approach that is both technically robust and scalable across the European Union by leveraging existing quality assurance expertise while incorporating targeted cybersecurity competence where required.

4. ISO 9001 and Module H are complementary, not equivalent

ISO 9001 can provide the management-system foundation for Module H, but it does not by itself demonstrate conformity with the CRA. Module H adds regulatory oversight, product-specific evidence and assessment against the applicable essential cybersecurity requirements.

ISO 9001-based Quality Assurance System (QAS)	CRA Module H Quality Assurance System (QAS)
Nature: Voluntary certification	Nature: Regulatory conformity assessment procedure under the CRA
Demonstrates that the manufacturer operates an effective Quality Assurance System	Demonstrates that the manufacturer's Quality Assurance System supports compliance with the CRA
Covers generic organisational processes.	Covers generic organisational processes and product-specific conformity with the CRA Essential Cybersecurity Requirements
Independent certification by an accredited certification body	Assessment by an EU Notified Body
Certification body focused on ISO 9001 requirements	Prerequisite: Rely on an ISO 9001 existing QAS evaluation - Notified Bodies rely on appropriate cybersecurity standards and technical specifications (e.g. ISO/IEC 27000 family, IEC 62443, ETSI EN 303 645, ETSI TS 103 701, EN 18031-1/-2/-3, where applicable) when assessing compliance with the CRA. - Assesses the manufacturer's process for determining product intended use, cybersecurity risks and security measures, supported by representative product evaluations. - Verifies the implementation of product security requirements (e.g. authentication, access control and other applicable Essential Requirements). - Assesses conformity using applicable harmonised standards, common specifications or other appropriate technical evidence under the CRA. - Reviews technical documentation and evidence demonstrating conformity of representative products.
Does not confer CE marking rights	Can support CE marking under the CRA.

Fig. 3 - Complementary Roles of Product Assurance and Information Assurance in Supporting CRA Compliance



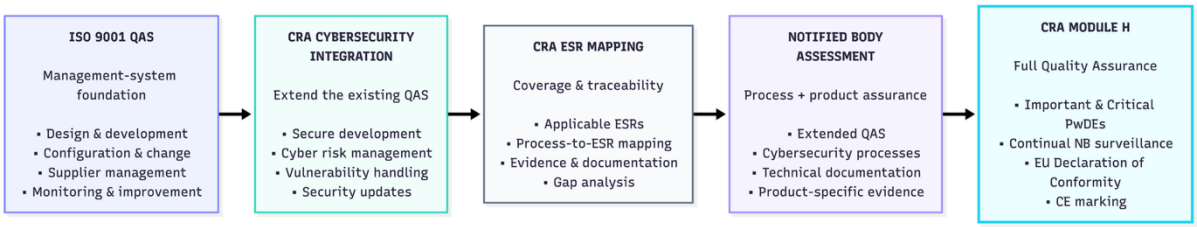
Conclusion:

The CRA introduces a lifecycle approach to cybersecurity that combines product requirements with engineering processes. Conformity assessment procedures based on Module H reflect this approach by evaluating both the manufacturer's assurance system and the evidence demonstrating product compliance.

For manufacturers operating an ISO 9001 Quality Assurance System, this provides a practical framework for integrating the cybersecurity processes required by the CRA into existing engineering and quality assurance practices. The Eurosmart Guide to Full Quality Assurance for CRA Conformity Assessment supports the consistent implementation of this approach by manufacturers and notified bodies.

This scalability will be essential for the effective implementation of the CRA, particularly for manufacturers of Important and Critical PwDEs managing large product families, extensive portfolios and legacy products. Building Module H conformity assessment on established ISO 9001 quality assurance practices, **complemented by the cybersecurity processes and product-specific evidence required by the CRA**, offers a pragmatic way to reuse mature industrial practices, avoid unnecessary duplication and make efficient use of Notified Body capacity. This will be important to support a timely roll-out of CRA conformity assessment without creating unnecessary discontinuity for products placed on the Union market.

Fig. 4 - From ISO 9001 Quality Assurance to CRA Module H: combining process assurance and product-specific evidence



Join Eurosmart shaping digital security standards and legislations

Eurosmart extends a warm invitation to all interested parties to join us in our pivotal mission to influence, promote, and advise on legislative frameworks concerning digital security standards and certifications. As we advocate for robust regulatory measures, the support of industry partners is paramount to our success. Whether your operations are within Europe or beyond, your collaboration is vital in bolstering our collective efforts towards fostering a secure digital environment.

Membership with Eurosmart offers the opportunity to contribute to impactful initiatives, providing access to an esteemed network of professionals, exclusive resources, and strategic partnerships. By aligning with Eurosmart, members gain a platform to actively participate in discussions, shape policies, and drive positive change in the realm of cybersecurity standards.

In navigating the complexities of evolving regulations, your partnership plays a pivotal role in advancing our shared objectives. Together, let us uphold the best regulatory and technical approaches, ensuring a safer digital future for all.

EUROSMART
The Voice of the Digital Security Industry

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