TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CRA-Module B and H: CABs accreditation for notification

Gap analysis for Module B and Module H vs RED and EUCC

NOVEMBER 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at: www.enisa.europa.eu.

CONTACT
To contact the authors, please use certification@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS
ENISA

LEGAL NOTICE
This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) 2019/881.
ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and must be accessible free of charge. All references to it or its use as a whole or in part must acknowledge ENISA as its source.
Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE
© European Union Agency for Cybersecurity (ENISA), 2026
Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/).

This means that reuse is allowed, provided appropriate credit is given and any changes are indicated.

Copyright for the image on the cover: © Adobe Stock
For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-820-4, DOI 10.2824/7808161

Table of Contents

1 Introduction 7
1.1 Background 7
1.2 Relevant Standards 7
1.3 Relevant Legislation 9
2 Key Findings 10
2.1 From RED to CRA-Module B 11
2.2 From EUCC to CRA-Module B 15
2.3 Module B: Conformity Assessment Activity Comparison 19
2.4 From RED to CRA-Module H 20
3 Scope and Approach 22
4 Notification Requirements and Their Accreditation Basis 24
5 CRA-Module B: CAB Technical Competences 30
5.1 Scope Of Accreditation 30
5.2 Standards for Accreditation for Notification 30
5.3 Competence Requirements for CRA-Module B Notified Bodies 31
5.4 Competence Requirements by Conformity Assessment Activity 33
5.4.1 Documentation and Design Review 33
5.4.2 Functional Security Testing 34
5.4.3 Configuration and Settings Inspection 35
5.4.4 Vulnerability Analysis 35
5.4.5 Assessment and testing of cryptographic mechanisms 36
5.4.6 Physical and Hardware Security Testing 36
5.4.7 Code and Binary Analysis 37
5.4.8 Process and Lifecycle Assessment 37
5.4.9 Examination of Vulnerability Handling and Reporting 38
5.4.10 Compliance Mapping and Evidence Aggregation 38
6 RED-Module B: CAB Technical Competences 40
6.1 Scope of Accreditation 40

6.2 Standards for Accreditation for Notification 41
6.3 Competence Requirements for RED-Module B Notified Bodies 41
6.4 Competence Requirements by Conformity Assessment Activity 42
6.4.1 Documentation and Conceptual Review 42
6.4.2 Functional Security Testing 43
6.4.3 Configuration and Default-State Inspection 44
6.4.4 Vulnerability Analysis 44
6.4.5 Cryptographic Validation 44
6.4.6 Physical and Hardware Security Testing 45
6.4.7 Code and Binary Analysis 45
6.4.8 Process and Lifecycle Assessment 45
6.4.9 Examination of Vulnerability Handling and Reporting 45
6.4.10 Compliance Mapping and Evidence Aggregation 46
6.5 RED – CRA Module B Gap Analysis and Competence Comparison 46
6.6 IT Security Assessment Capability Gap Analysis: CRA and RED 47
6.6.1 Capabilities Required by CRA But Absent from RED 47
6.6.2 Capabilities Required by RED but Absent from CRA Vertical Standards 48
6.6.3 Capabilities Required by both Frameworks with Material Scope Differences 49
6.6.4 Qualification Gap Synthesis 50
7 EUCC: CAB Technical Competences 52
7.1 Scope of Accreditation 52
7.2 Standards for Accreditation for Notification 53
7.3 Competence Requirements for EUCC CABs (CBs and ITSEFs) 53
7.4 Competence Requirements by Conformity Assessment Activity 55
7.4.1 Security Target evaluation (ASE) 55
7.4.2 Design and architecture review (ADV) 56
7.4.3 Guidance review (AGD) 56
7.4.4 Lifecycle and process assessment (ALC) 56
7.4.5 Functional security testing (ATE) 57
7.4.6 Vulnerability analysis and penetration testing (AVA) 57
7.4.7 Cryptographic assessment 57
7.4.8 Patch management assessment 57
7.4.9 Compliance mapping and certification review 58
7.4.10 Technology-specific competence areas 58
7.5 EUCC – CRA Module B Gap Analysis and Competence Comparison 59
7.6 IT Security Assessment Capability Gap Analysis: CRA and EUCC 61
7.6.1 Requirement-by-Requirement Bridge and Gap Assessment 61
7.6.2 CRA Areas With No EUCC Bridge at Substantial Level 68
7.6.3 Qualification Gap Synthesis 70

7.7 EUCC Certificates as Evidence of CRA Conformity 71

8 CRA-Module H: CAB Technical Competences 72

8.1 Scope of Accreditation 72
8.2 Standards for Accreditation for Notification 73
8.3 Competence Requirements for CRA-Module H Notified Bodies 74

9 RED-Module H: CAB Technical Competences 77

9.1 Scope of Accreditation 77
9.2 Standards for Accreditation for Notification 78
9.3 Competence Requirements for RED-Module H Notified Bodies 78
9.4 RED – CRA Module H Gap Analysis and Competence Comparison 80

List of Figures

Pages

Figure 1. Notification and Accreditation Basis, by Framework and Module 26
Figure 2. Notification Requirements for Module B 29
Figure 3. Annex C – EA Accreditation for Notification (AfN) Project Report..... 31

List of Tables

Pages

Table 1. Identified Competence Gaps for RED-Accredited Bodies in CRA-Module B evaluations..... 13
Table 2. Identified Competence Gaps for EUCC-Accredited ITSEFs in CRA-Module B evaluations... 16
Table 3. Conformity Assessment Activity Comparison, CRA-Module B vs RED-Module B vs EUCC .. 19
Table 4. Notification and Accreditation Basis, by Framework and Module..... 24
Table 5. Notification Requirements for Module B 27
Table 6. CRA-Module B: Specific requirements related to the scope of accreditation..... 31
Table 7. CRA-Module B: Specific requirements related to the type of conformity assessment activity 32
Table 8. CRA-Module B: Structural and process requirements..... 33
Table 9. RED-Module B: Specific requirements related to the scope of accreditation..... 41
Table 10. RED-Module B: Specific requirements related to the type of conformity assessment activity 41
Table 11. CRA and RED-Module B CAB Competence and Accreditation Requirements 46
Table 12. EUCC: Specific requirements related to the scope of accreditation..... 54
Table 13. EUCC: Specific requirements related to the type of conformity assessment activity..... 54
Table 14. EUCC – CRA Module B: Competence and Accreditation Mapping..... 60
Table 15. CRA–EUCC Mapping of CAB Technical Competence Requirements and Qualification Gaps 61
Table 16: CRA Areas With No EUCC Bridge at Substantial Level 68
Table 17. CRA-Module H: Specific requirements related to the scope of accreditation 74
Table 18. CRA-Module H: Specific requirements related to the type of conformity assessment activity 74
Table 19. CRA-Module H: Structural and process requirements 75
Table 20. RED-Module H: Specific requirements related to the scope of accreditation 78
Table 21. RED-Module H: Specific requirements related to the type of conformity assessment activity 79
Table 22. RED-Module H: Structural and process requirements (identical to Section 8.3) 79
Table 23. RED–CRA Module H CAB Competence and Accreditation Requirements (Gap Comparison) 80

1 Introduction

1.1 Background

The Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847[1]) introduces conformity assessment and notification requirements for products with digital elements, following the New Legislative Framework (NLF) model already applied under Radio Equipment Directive (RED) (Regulation (EU) 2014/53[2]) and other EU product legislation.

ENISA was tasked, in support of the Commission's implementation of the CRA, with a gap analysis comparing the accreditation and notification requirements for CRA notified bodies with those already established for RED Notified Bodies and the European Common Criteria-based cybersecurity certification scheme (EUCC) as well as certification bodies (CBs) and IT Security Evaluation Facilities (ITSEF testing laboratories), focusing on the technical competences that conformity assessment bodies (CABs) need to obtain notification.

This document is a non-binding technical reference intended to support notifying authorities and national accreditation bodies in assessing the competence of CABs for the assessment of conformity with the requirements of the CRA. It identifies relevant existing competence and additional CRA-specific requirements, with the aim of supporting consistent and efficient assessment. It does not determine accreditation or notification eligibility; each CAB must demonstrate compliance with the applicable CRA requirements for its requested scope.

This document addresses **four questions.**

1) What accreditation regime and standard(s) apply to each framework?
2) What technical competences does each framework require of a CAB?
3) How does each framework define the scope of products for which a CAB may be notified?
4) Where does a RED- or EUCC-based CAB's existing competence already align with what the CRA requires, and where it falls short?

The analysis examines both the assessment procedures for conformity with the CRA that rely on a notified body – **Module B** (EU-type examination) and **Module H** (full quality assurance) – against their RED and, where applicable, EUCC equivalents.

1.2 Relevant Standards

Accreditation and conformity assessment standards (ISO/IEC)

- **ISO/IEC 17065:2012** – requirements for bodies certifying products, processes and services. The common accreditation basis across CRA, RED and EUCC certification bodies.
- **ISO/IEC 17025:2017** – general requirements for the competence of testing and calibration laboratories. Applies to CRA and EUCC testing activities; not applicable to RED Notified Bodies.
- **ISO/IEC 17020:2026**, clauses 6.1.2–6.1.3 and 6.1.6–6.1.10 – competence requirements for inspection bodies, applied to the assessment of the vulnerability-handling processes of manufacturers under the CRA. The international transition period (from the ISO/IEC 17020:2012) is three years for the accreditation of CABs.
- **ISO/IEC 17021-1:2015** – requirements for bodies auditing and certifying management systems. The preferred accreditation basis for Module H (CRA and RED), covering the assessment of a manufacturer's quality control system.

[1] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053.

- **ISO/IEC 27006-1:2024** – additional requirements for bodies auditing and certifying information security management systems (ISMS). It is relevant to competence for an ISO/IEC 27001-based approach; it is not a universal CRA Module H requirement.
- **ISO 9001:2015** – requirements for quality management system. It may support a manufacturer's Module H quality system. Separately, ISO 9001 provides an alternative framework (Option B) for the CAB's own quality management system under ISO/IEC 17065 or ISO/IEC 17021-1.
- **ISO/IEC 27001:2022** and **ISO/IEC 27002:2022** – requirements for an information security management system and guidance on supporting control. An ISO/IEC 27001-based system may support CRA Module H where it is extended to cover the relevant processes for product design, development, production and vulnerability handling.
- **BSI TR-03183-H, version 1.1.0** – conformity based on full quality assurance (Module H). Describes CRA-specific refinements and additions to ISO/IEC 27001 requirements and associated ISO/IEC 27002 guidance. [BSI Technical Guideline[3]].

For the manufacturer, the governing criteria are CRA Annex VIII, Part IV. Neither ISO 9001 nor ISO/IEC 27001 certification is mandatory or sufficient by itself. The quality system must meet all applicable Module H requirements and remains subject to assessment, approval and surveillance by a notified body. These implementation frameworks are distinct from the basis of a CAB's accreditation.

EA-2/17 M:2026 and its supplements[4] govern the EA approach to accreditation for notification. Supplement 1 (mandatory) sets the obligatory harmonised standard and obligatory requirements for non-aligned legislation, including CRA Annex VIII, Part II (Module B) and Part IV (Module H). Supplement 2 (informative) provides examples of scopes of accreditation (including CRA). The documents were published on 25 June 2026, with implementation by National Accreditation Bodies (NABs) within one year for new or revised requirements. This approach uses the terms *obligatory HS* and *obligatory requirements*.

Evaluator and reviewer competence standards

- **ISO/IEC 19896-1:2025** and **ISO/IEC 19896-3:2025 –** personnel-competence requirements for IT security evaluations and reviews. Part 3 applies specifically to evaluators and reviewers working under ISO/IEC 15408 and ISO/IEC 18045 and is therefore relevant to ITSEF evaluators, EUCC certification-body reviewers and, where those methodologies are used, CRA notified-body personnel. **ISO/IEC TS 23532-1:2021** provides additional operational guidance for Common Criteria testing laboratories.

Vulnerability handling and disclosure standards

- **ISO/IEC 30111:2019** and **ISO/IEC 29147:2018** – vulnerability handling and vulnerability disclosure processes, referenced for CRA Annex I, Part II assessment.

EUCC scheme and Common Criteria standards

- **ISO/IEC 15408:2022** – Common Criteria (Parts 1–3).
- **ISO/IEC 18045:2022** – Common Evaluation Methodology (CEM).
- **ISO/IEC TS 9569** – patch-management evaluation criteria; proposed by ENISA as the reference for EUCC patch mechanism for Security Assurance Requirements (SARs).

Harmonised standards supporting the RED cybersecurity essential requirements

- **EN 18031-1:2024** – network protection (RED Art. 3.3(d)).
- **EN 18031-2:2024** – privacy safeguards (RED Art. 3.3(e)).
- **EN 18031-3:2024** – protection from fraud (RED Art. 3.3(f)).

[3] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-H_v1_1_0.pdf?__blob=publicationFile&v=3.
[4] European co-operation for Accreditation, EA-2/17 M:2026 (25 June 2026), Sections 3–5 and Annex A; EA-2/17 S1 M:2026, CRA entries and Key; EA-2/17 S2:2026, informative scope examples. Main document: https://european-accreditation.org/wp-content/uploads/2025/10/ea-2-17-m.pdf; Supplement 1: https://european-accreditation.org/wp-content/uploads/2026/06/EA-2_17-S1.pdf; Supplement 2: https://european-accreditation.org/wp-content/uploads/2026/06/EA-2_17-S2.pdf.

CRA harmonised standards under development (Standardisation Request M/606)

- **prEN 40000 horizontal series** – CRA standards under development, covering vocabulary (prEN 40000-1-1), cyber-resilience principles (prEN 40000-1-2) and vulnerability handling requirements in CRA Annex I, Part II (prEN 40000-1-3).
- **ETSI EN 304 6xx series** – CRA vertical (product-specific) standards under development, under standardisation request M/606.
- **prEN 40000-1-10** – Essential cybersecurity requirements for products - Part 10: draft vertical standard for products with digital elements used in identity-management systems and privileged-access management software and hardware, including biometric readers.
- **prEN 40000-1-11** – Essential cybersecurity requirements for products - Part 11: draft vertical standard for Hardware Devices with Security Boxes incorporating a hardware-physical envelope and designed to provide security functions such as secure storage and cryptographic operations in open environments.

Note: These draft standards are referenced solely to identify emerging product-specific assessment activities and anticipated needs for CAB competence. In accordance with EA TMB Resolution 2026 (25) 01, *draft standards cannot be used as normative accreditation criteria or referenced as such in the scope of accreditation. For level 5 standards, a draft standard might be referenced in the scope of accreditation only as a CAB's developed and validated method or procedure*. Once formally approved and published, the standards may be considered for accreditation purposes; presumption of conformity under the CRA additionally depends on their citation in the Official Journal.

1.3 Relevant Legislation

- **Regulation (EU) 2024/2847** – the Cyber Resilience Act (CRA).
- **Directive 2014/53/EU** – the Radio Equipment Directive (RED).
- **Commission Delegated Regulation (EU) 2022/30** – supplements RED Article 3(3)(d)(e)(f) and specifies the radio equipment product categories within the scope of the directive.
- Commission Implementing Regulation (EU) 2024/482 – establishes the EUCC scheme.
- **Commission Implementing Regulation (EU) 2025/2462** – second amendment to the EUCC Implementing Regulation (8 December 2025): definitions, ICT product series certification, assurance continuity, updated state-of-the-art (SotA) documents.
- **Regulation (EU) 2019/881** – the Cybersecurity Act (CSA), the legal basis for EUCC and for ENISA's role in cybersecurity certification.
- **Regulation (EC) No 765/2008** – sets the general framework for accreditation and market surveillance and establishes accreditation as the preferred basis for assessing the competence of CABs.
- **Decision No 768/2008/EC** – the common framework for the marketing of products (NLF template), setting the standard criteria for notified bodies referenced by both CRA and RED.

Application timeline and RED transition. CRA Chapter IV has been applied since 11 June 2026, while Article 14 has been applied since 11 September 2026. The CRA will be applicable in full as of 11 December 2027. From that date, Commission Delegated Regulation (EU) 2022/30 will be repealed by Commission Delegated Regulation (EU) 2026/339, and products placed on the market before that date remain subject to the requirements of RED cybersecurity. The RED-to-CRA analysis should therefore be read as an assessment of the capacity of bodies currently active under the scope of RED cybersecurity to qualify for CRA notification, but not as a transfer of status since CRA notification is a separate process. The EN 18031 series remain subject to the limitations attached to its citation by Commission Implementing Decision (EU) 2025/138. These restrictions determine whether reliance on the harmonised standards provides a presumption of conformity and so avoids the involvement of notified bodies under the RED.

2 Key Findings

All three frameworks (CRA, RED, EUCC) share a **common foundation in Regulation (EC) No 765/2008,** CRA and RED treat accreditation treat accreditation as the *preferred means of demonstrating technical competence*[5]. EUCC adds an additional authorisation layer for high-assurance activities, which has no equivalence in CRA or RED.

Under the CRA (Module B), conformity assessment bodies (CABs) and notified bodies apply **ISO/IEC 17065** to product certification processes and use the appropriate Level-3 standards such as **ISO/IEC 17020** and **ISO/IEC 17025** to assess compliance with Annex I, Part I essential requirements. Under the EUCC, **ISO/IEC 17065** applies to CBs while **ISO/IEC 17025 applies** to Information Technology Security Evaluation Facilities (ITSEFs) performing testing and evaluation activities. Consequently, EUCC provides a strong baseline as there are already EUCC-CABs accredited according to ISO/IEC 17065. The technical competences of the ISO/IEC 17025 ITSEFs might be useful for addressing some of the requirements for product security in **CRA Annex I, Part I**.

A RED Module B notified body or an EUCC certification body accredited under ISO/IEC 17065 may reuse existing organisational and certification-system evidence where it is demonstrably relevant to the requested CRA scope. The requirements concerning independence, impartiality, liability, confidentiality and control of subcontracting are substantially aligned. However, their application must be reviewed against CRA activities, risks and arrangements. Existing evidence may support the assessment, while CRA-specific adaptations and competence must still be demonstrated. Existing accreditation or notification does not confer automatic eligibility for CRA notification.

EUCC-accredited certification bodies, supported by appropriately scoped ITSEFs or operating within a combined CB/ITSEF structure, may provide one of the most direct routes to CRA Module B notification, subject to closing the remaining CRA-specific organisational and technical gaps. Their combined certification and evaluation competence overlaps substantially with CRA Module B requirements, and the remaining gap may be moderate where the relevant scope of the product and technical competences are already covered. EUCC is not restricted to a closed list of product categories. The relevant limitations are the body's demonstrated scope in technology, and the defined evaluation boundary and applicable requirements of the target of evaluation (TOE). CRA covers a substantially broader range of product categories than the EUCC. Extending coverage to the 20+ product families and emerging vertical standards (ETSI and (partly) CEN) poses a huge challenge to testing laboratories, as it may require significant investment in testing methods, tools and personnel. Depending on the requirement, the remaining differences must be addressed according to their nature and the body's existing scope of accreditation.

RED-Module H bodies are close to CRA-Module H notification already. The frameworks share ISO/IEC 17021-1 as the preferred accreditation basis and are substantially aligned structurally. The principal remaining **gaps are CRA-specific** assessment of development and vulnerability-handling controls within the quality system, **and extension of product-specific** competence to assess design controls against CRA Annex I, Part I and the applicable technical specifications. This concerns the approved quality system and product conformity; it does not establish a general requirement to operate or certify an SDLC.

RED-Module B bodies face the largest gap. This finding applies particularly to the **testing laboratories supporting RED conformity assessment that currently perform only EN 18031 assessments**, rather than exclusively to the notified bodies themselves. Closing it is not a matter of incremental upskilling: it requires additional product-security testing and competence to assess relevant product-development evidence and manufacturer vulnerability-handling processes. **EUCC ITSEFs have a stronger existing competence base**, because lifecycle-related processes are addressed by customer experience management (CEM) through the ALC assurance class. However, this competence does not automatically cover the complete CRA Annex I, Part II

[5] Regulation (EC) No 765/2008, Recital 12.

framework; the remaining gap depends on the ITSEF's accredited scope and the ALC components for which it has demonstrated competence. In practice, this also means that manufacturers with diverse product portfolios cannot assume their existing RED Notified Body will be able to certify all of their CRA products without that body first closing this gap.

The CRA Module B assessment model has implications beyond the initial certification decision. Because CRA Module B extends assessment to manufacturing processes and product lifecycle, not just the product as built, the **notified body's role does not end with the issuance of the EU-type examination certificate**. A **periodic audit** must be performed to assess whether the manufacturer's vulnerability-handling processes are being adequately implemented. It must also **assess changes** to the approved type of vulnerability-handling processes that may affect conformity or certificate validity. Depending on the product, risks and applicable assessment requirements, these activities may involve examining relevant development, build or CI/CD evidence. This does not establish a general SDLC assessment duty; periodic process audits concern Annex I, Part II vulnerability handling. These periodic-audit and certificate-maintenance obligations are comparable to elements associated with a Type 5 product-certification scheme under ISO/IEC 17067. The EUCC does not provide equivalent periodic surveillance of the manufacturer's complete CRA framework for handling vulnerabilities. This is a methodological comparison only: neither the CRA nor the applicable EA documents formally classify CRA Module B as a Type 5 scheme.

Disclaimer. This analysis is an ENISA technical and comparative assessment aimed to support policy and capacity-planning discussions. It does not constitute formal legal or technical advice and should not be treated as a definitive determination of compliance or eligibility under the CRA, RED, EUCC, accreditation legislation or any other regulatory or accreditation framework. In particular, the conclusions should not be used as a substitute for an assessment by the competent notifying authority or National Accreditation Body of the applicable legal and accreditation requirements.

The sections below present the detailed findings and a synthetic comparison table.

This report examines four transition paths:

1. RED Module B notified bodies to CRA Module B;
2. EUCC certification bodies accredited under ISO/IEC 17065 to CRA Module B;
3. EUCC ITSEFs accredited under ISO/IEC 17025 to CRA Module B;
4. RED Module H notified bodies to CRA Module H.

No separate EUCC-to-CRA Module H comparison is performed. EUCC is a product-certification scheme based on ISO/IEC 17065 for certification bodies and ISO/IEC 17025 for ITSEFs, whereas CRA Module H concerns full-quality assurance and management-system assessment, for which ISO/IEC 17021-1 is the preferred accreditation basis. The EUCC therefore has no directly comparable Module H procedure or existing accreditation route to assess.

2.1 From RED to CRA-Module B

Of the four CAB transition paths assessed in this study, this presents the largest gap. A RED Module B notified body accredited under ISO/IEC 17065 can largely reuse its existing organisational evidence when applying for CRA notification. However, RED accreditation does not automatically demonstrate compliance with the CRA. One should be aware that this is only true for existing 17065-accreditations and that the requirements need to be adjusted regarding the new context. The **remaining gap is therefore both structural and technical**.

- **The assessment framework differs.** EN 18031 (the harmonised standard for the essential requirements for RED's cybersecurity) requires a mechanism-by-mechanism assessment with three formal tiers (conceptual, completeness, sufficiency) and pass/fail verdicts tied to

decision trees. CRA Module B requires examination of the product's technical design and development, technical documentation, supporting evidence and specimens, together with the manufacturer's processes for handling vulnerabilities (Annex VIII, Part II, points 1–4). The CRA does not prescribe one testing methodology or require assessment to be organised by testing-capability category.

- **The scope of what is assessed differs.** RED Module B and EN 18031 focus on the radio equipment and its security mechanisms. CRA Module B additionally examines the adequacy of its technical design and development against Annex I, Part I and the manufacturer's processes for handling vulnerabilities compared to Annex I, Part II. Annex I, Part I (1) concerns identified cybersecurity risks, particularly risks not adequately addressed by the other Part I requirements; it does not require the manufacturer to operate an SDLC (Commission CRA guidance[6], section 7.2, paragraphs 164 – 166). Relevant development evidence may support product conformity assessment, but the notified body does not assess whether the manufacturer has an SDLC. Periodic audits concern implementation of the vulnerability-handling processes (Annex VIII, Part II, point 8). The vulnerability-handling element has no direct counterpart in RED conformity assessment.

Several technical competence areas would need to be developed.

- **Code and binary analysis**. Source code review, binary hardening verification (CRA Annex I, Part I(1), (2)(a), (k), Part II (3)).
- **Product-development evidence and vulnerability-handling process assessment**: review of evidence supporting conformity of the product's technical design and development with Annex I, Part I, and assessment of the manufacturer's vulnerability-handling processes under Annex I, Part II, including monitoring, remediation and SBOM-related evidence. This does not require assessment of whether the manufacturer operates an SDLC. Periodic audits cover vulnerability-handling process implementation (CRA Annex VII; Annex VIII, Part II, points 1, 4.1 and 8).
- **Physical and hardware security testing.** Where justified by the product category, intended purpose and expected use, the manufacturer's cybersecurity risk assessment, the product's attack surface and the applicable technical specifications, including where relevant physical attack vectors are identified, competence in debugging interface security is required, along with the ability to handle physical tampering and specialised hardware-attack techniques (CRA Annex I, Part I(2)(d), (j) and (k)).
- **Isolation and containment testing.** Process isolation, sandboxing and container/virtual machine (VM) separation (CRA Annex I, Part I(2)(k)).
- **Data minimisation assessment**. Assessment as to whether the personal and other data processed by the product are adequate, relevant and limited to what is necessary for its intended purpose (CRA Annex I, Part I(2)(g)). EN 18031-2 provides a related competence base through the protection of personal data and the minimisation of logged information. The extension needed depends on the CAB's existing scope and demonstrated competence.
- **Vulnerability analysis methodology**. The selection and application of appropriate product-level methods for the analysis of vulnerabilities, building on checks in EN 18031 GEC-1 for publicly known exploitable vulnerabilities, is required. The methods and depth, including penetration testing where justified, depend on product risks, applicable standards or specifications and the notified body's assessment procedures. The CRA prescribes no single method (Annex I, Part I(2)(a) and, where relevant, (j) and (k)).
- **Support-period documentation review.** Verification is required that the manufacturer has documented the information used to determine the support period in the technical documentation and has clearly communicated the end date of that period to users and, where

[6] Commission publishes new guidance to support timely Cyber Resilience Act implementation, 27 July 2026, Available from: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation

technically feasible, can notify users when the product reaches the end of its support period (CRA Article 13(8), Annex VII and Annex II (CRA Art. 13(8) and (19)).

Closing these gaps requires a **combination of extending** existing RED evaluation **competence and establishing additional capabilities** where the requested CRA scope requires them. The assessment of vulnerability and security mechanisms in EN 18031 provide a foundation for some activities. Analyses of source code and an assessment of the manufacturer's process for handling vulnerabilities may require separate methods, tools or personnel competence. The extent of development needed must be determined for the individual CAB and its requested scope.

For the comparison of technical competence, the following qualitative gap levels are used:

- **None** – existing evaluation competence directly covers the requirement;
- **Low** – the requirement extends an existing competence and requires limited familiarisation or scheme-specific interpretation;
- **Medium** – the requirement introduces a materially new domain of knowledge or evaluator judgement for which dedicated competence development such as training, guidance and scheme-level harmonisation are needed;
- **High** – the requirement involves skills, tools or expertise fundamentally outside the evaluation paradigm.

Table 1. Identified Competence Gaps for RED-Accredited Bodies in CRA-Module B evaluations

COMPETENCE	GAP LEVEL	ENISA ASSESSMENT RATIONALE
Code and binary analysis (CRA Annex I, Part I (2)(a) and Part II (1))	High	RED-Module B has no equivalent activity (see 6.4). A RED notified body qualified only for EN 18031 would have no directly equivalent competence within its existing RED scope. It would therefore need to establish or separately demonstrate the necessary capabilities in source-code and binary analysis.
Manufacturer development and vulnerability-handling process assessment (CRA Article 13(2); Annex I, Part I (1) and Part II; Annex VIII, Part II, points 1, 4.1 and 8)	High	RED Module B has no equivalent to assessment and periodic auditing of the complete CRA vulnerability-handling framework (see 6.4). Additional competence is needed to assess those processes and relevant evidence supporting product conformity. The CRA does not require an SDLC, and the notified body does not assess whether one exists. Periodic audits under Module B concern vulnerability-handling implementation.
Isolation and containment testing (CRA Annex I, Part I(2)(k))	High	EN 18031 does not prescribe process-isolation, sandboxing or container/VM-separation testing as distinct assessment activities. Although a RED NB's existing competence in security-mechanism assessment provides a limited foundation, it would need to develop or demonstrate product-specific methods, tools and expertise where isolation or containment mechanisms are used to satisfy CRA product-specific requirements (Annex I, Part I(2)(k)).

Data minimisation assessment (CRA Annex I, Part I(2)(g))	Medium-High	EN 18031-2 provides a relevant competence base, including the handling and protection of personal data and data minimisation in logging. However, CRA requires a broader assessment of whether data processing is limited to what is adequate, relevant and necessary for the product's intended purpose. The gap is **Medium** for CABs qualified under EN 18031-2 as extending their existing privacy-related assessment competence to this necessity-based judgement requires additional competence development. The gap is **High** for CABs whose RED scope does not include EN 18031-2, as they lack this existing competence base.
Physical and hardware security testing (CRA Annex I, Part I(2)(d), (j) and (k) where applicable)	Medium-High	EN 18031 provides a limited, scope-dependent competence through secure-update, secure-storage assessments. Boot-integrity competence is limited to CABs whose scope includes RED Article 3(3)(f) and EN 18031-3. CRA does not require physical or hardware security testing for every product. Such testing may be necessary depending on the product category, intended purpose and environment in which it is used, the manufacturer's cybersecurity risk assessment, the product's attack surface and the applicable technical specifications. Where relevant physical attack vectors are identified, the assessment may extend to the security of the debugging interface, tamper resistance or specialised techniques on hardware attacks. These fall outside the scope of EN 18031 and may require additional methods, equipment and personnel competence. The gap is **Medium** where relevant competence already exists. The gap is **High** where a CRA assessment requires specialised debug-interface, fault-injection or tamper-resistance testing outside its existing scope.
Support-period documentation review (CRA Art. 13(8), (19); Annex II and Annex VII)	Medium	The CRA requires manufacturers to determine and communicate the product's support period and make security updates available throughout that period. RED Module B has no comparable support-period regime; its continuing obligations concern modifications to the approved type and developments in the state-of-the-art. Assessing a documented support period and its justification does not require new technical skills or tools. Relevant competence concerns reviewing the information on the support period contained in the technical documentation and user information and its consistency with the evidence of conformity.
Vulnerability analysis methodology (CRA Annex I, Part I(2)(a) and, where relevant, (j) and (k))	Medium	EN 18031 provides a limited competence base through GEC-1 checks for publicly known exploitable vulnerabilities. CRA assessment may require broader product-level analysis, with the methods and depth determined by product risks, applicable standards or specifications and the notified body's justified procedures. The additional competence concerns selecting and applying appropriate methods, including

		penetration testing where needed; the CRA does not prescribe a single methodology for analysing vulnerabilities.

Section 6.6 (IT Security Assessment Capability Gap Analysis: CRA and RED) analyses the differences in testing capabilities and qualification requirements between CABs assessing products under the CRA and those operating under RED, identifying capability gaps, common areas with material differences in scope, and the resulting additional qualification needs.

2.2 From EUCC to CRA-Module B

This is a moderate, well-bounded gap, with **the extent of the gap depending on the CB/ITSEF arrangement, its demonstrated competences and the applicable product and scope of evaluation. EUCC CBs** accredited under ISO/IEC 17065 have an established organisational and certification-system foundation relevant to CRA Module B. However, they must adapt their procedures and documentation to the CRA context and demonstrate competence for the requested CRA accreditation and notification scope. Depending on their accredited scope, technology coverage and demonstrated evaluation techniques, **EUCC ITSEFs** accredited under ISO/IEC 17025 may provide relevant competence for some of the underlying IT-security evaluation and testing activities required by CRA Module B. However, ITSEF accreditation alone does not demonstrate competence to perform the complete CRA Module B procedure.

The evaluation boundary also matters. EUCC addresses the Target of Evaluation (TOE), its evaluated configuration and the security requirements defined in the Security Target, which may cover only part of a product. CRA Module B must address the product (with digital elements) as placed on the market and all applicable Annex I requirements. This includes *remote data processing solutions* only where they meet Article 3(2) criteria. EUCC evidence must therefore be mapped to the CRA product boundary, with any uncovered components, functions or qualifying remote processing assessed additionally (CRA Article 3(1)–(2)).

For an ITSEF to qualify independently as a CRA notified body capable of performing the complete Module B procedure, two **major cross-cutting gaps** must be addressed.

1. **Competences** in **organisational matters, management systems, reviews and independent decision-making certification required by ISO/IEC 17065:2012** that are not covered by its ISO/IEC 17025 accreditation must be established or demonstrated. In the EUCC model these fall under the CB.
2. For extensions of the ITSEF's existing **Common Criteria lifecycle support, flaw remediation and monitoring competences** to cover the manufacturer's **processes in handling vulnerabilities** in the CRA Annex I, Part II and the **periodic audits** under Annex VIII, Part II, including the applicable ISO/IEC 17020 competence requirements, particularly clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10, separate ISO/IEC 17020 accreditation is not necessarily required. **Site audits** fall outside the intended scope of ISO/IEC 17025, but ITSEFs already perform them in practice, and the competence is present in ITSEFs that evaluate from EAL3 upwards. It cannot be assumed for ITSEFs working only at lower assurance levels.

Where an EUCC CB uses an appropriately accredited ITSEF as an evaluation resource, the two organisations may collectively provide the required foundation. The CRA notified body however retains responsibility for the evaluation review and the final decision on Module B certification.

Despite these structural differences, EUCC and CRA show **substantial technical overlap in several areas**, including cryptographic implementation, access control, integrity protection, vulnerability analysis and penetration testing. The analysis nevertheless identifies additional CRA-specific competences that may need to be established or extended, with the extent of the gap depending on

the ITSEF's existing scope of accreditation, technical domains, product and technology coverage, evaluation techniques and demonstrated personnel competence.

For the comparison of technical competence, the same qualitative gap levels used for the RED assessment are applied. The ratings assess transferable ITSEF personnel competence and additional qualification needs; they do not determine whether each activity falls within the scope of ISO/IEC 17025 accreditation. In accordance with EA TMB Resolution 2022 (09) 01, activities that are not being tested – including certain ALC lifecycle and process assessments, verifications of conformity to harmonised standards, risk-based design and risk-assessment reviews, and data-minimisation assessments – may need to be performed or controlled within the ISO/IEC 17065-accredited certification function. Related ITSEF competence should therefore be treated as a technical foundation, not as evidence that the complete CRA assessment activity is already covered by the ITSEF's accreditation.

The gap levels in Table 2 and Table 15 concern the additional competence needed for CRA Module B, taking account of the body's existing scope and the demonstrated competence of its personnel. Proposed extended components are used only as analytical mappings from the ENISA study; they do not establish current EUCC coverage, product-certificate equivalence or automatic eligibility for CRA notification.

Table 2. Identified Competence Gaps for EUCC-Accredited ITSEFs in CRA-Module B evaluations

COMPETENCE	GAP LEVEL	ENISA ASSESSMENT RATIONALE
Data minimisation review (ADV_PDM.1 – proposed extension)	Medium	ITSEF personnel may possess related competence in interface and data-flow analysis. However, CC/CEM does not generally require assessment of whether data processing is necessary or proportionate, and this activity cannot be presumed to fall within accreditation under ISO/IEC 17025. Additional knowledge of data-protection principles and the ability to make proportionality judgements on data processing are required, with the activity performed or controlled within the ISO/IEC 17065 certification function.
SBOM verification (ALC_SBM.1 – proposed extension)	Medium	ITSEF personnel may possess related component-analysis and flaw-remediation competence. However, ALC_SBM.1 introduces a new evidence type, and its assessment cannot automatically be treated as an ISO/IEC 17025 testing activity. Additional competence is required to assess machine-readable SBOMs and verify their completeness and consistency against the TOE, including familiarity with relevant formats (CycloneDX[7] 1.4 or higher or SPDX[8] 2.3 or higher) and tools.
Assessments of periodic security reviews (ALC_PSR.1 – proposed extension)	Medium	ITSEF personnel may have relevant experience in assessing developer procedures and completed security-testing activities under CC/CEM. The proposed ALC_PSR.1 extends this to evaluating a continuing, forward-looking security-testing programme. Since this is not purely a testing activity, it cannot be presumed to fall within ISO/IEC 17025 accreditation and may need to be performed or controlled within the ISO/IEC 17065 certification function.
Assessment of the effectiveness	Medium	Requires product-specific knowledge of data-destruction methods, media-remanence properties and, where applicable,

[7] OWASP; https://cyclonedx.org/.
[8] https://spdx.dev/.

of a decommissioning assessment (AGD_DEC.1 – proposed extension)		the physical security or destruction of end-of-life hardware. ITSEFs with relevant experience in evaluating hardware or storage security may already possess much of this competence, whereas software-focused ITSEFs may need to develop it. For software products, the assessment generally concerns secure deletion, removal of credentials and configuration data, and uninstallation rather than physical destruction.
Risk-based reviews of documentation on assessments of design or risk	Medium	ITSEF personnel may possess a partial analytical foundation through CC/CEM assessment of the Security Problem Definition, including threats, assumptions, organisational security policies and their traceability to security objectives and requirements. However, the risk analysis underlying the Security Problem Definition is ordinarily conducted outside the CC evaluation, and the ITSEF does not normally assess the manufacturer's complete cybersecurity risk assessment at the product level. Additional competence is therefore required in cybersecurity risk-assessment methodologies to determine whether the manufacturer's assessment is sound, complete and appropriate across the complete product and its lifecycle. The CRA does not prescribe a specific risk-assessment methodology, and the CAB assesses, rather than performs, the manufacturer's assessment. This broader completeness and applicability judgement cannot be presumed to be covered by the ITSEF's ISO/IEC 17025 accreditation and, where it extends beyond testing, should be performed or controlled within the ISO/IEC 17065 certification function. ITSEF personnel may contribute, where relevant, competence in risk assessment at the product level that has been separately demonstrated within the CAB.
DoS resilience testing (FRU_RSA.1/2)	Low–Medium	Relevant ITSEF experience in availability, the management of resources and evaluation of fault tolerances. CRA coverage depends on the evaluated requirements and product risks. Additional competence may be needed to design and execute product-specific DoS and resource-exhaustion tests using suitable load or traffic-generation tools. ITSEFs with experience in evaluating network products may already possess this competence.
Harmonised standard conformity verification	Low–Medium	ITSEF personnel have relevant competence in testing conformity using Automated Test Equipment (ATE), complemented by experience in assessing conformance with Security Target and Protection Profiles. This provides a strong foundation for testing whether a product satisfies the technical requirements of an applicable CRA harmonised standard. However, CRA Module B additionally requires verification that the standard has been correctly applied and covers the relevant essential requirements. Where the standard is not applied or provides only partial coverage, the CAB must assess alternative technical solutions directly against those requirements. The gap is **Low** for standards-based testing and verification, subject to the scope of the ITSEF's accreditation. The gap is **Medium** where alternative solutions require broader regulatory and engineering judgement. The final

		decision on conformity must be controlled by the ISO/IEC 17065-accredited body.
Secure default configuration review (ADV_ARC.2 – proposed extension)	Low	The proposed extension would extend existing ADV_ARC.1 analysis of security architecture to assess and justify the TOE's default security state as delivered, before any user configuration.
Secure update mechanism testing	Low	ITSEFs already possess relevant skills in the evaluation of patch management and competence in functional testing. The extension requires testing four CRA-specific properties not expressly covered by the existing EUCC patch-management framework: automatic updating by default, an accessible opt-out mechanism, user notification and temporary postponement. Limited CRA-specific familiarisation and scheme-level guidance should therefore be sufficient.
Permanent data-removal and secure-transfer assessment	Low	Relevant ITSEF experience in data protection, security management and secure communications provides a foundation for assessing user-controlled permanent deletion and secure transfer. Explicit coverage and effectiveness checks are needed, potentially including product-specific data-recovery techniques. This assumes that relevant deletion and transfer competence has already been demonstrated.
Flaw-separation review (ALC_FLR.4 – proposed extension)	Low	ITSEF personnel may possess related competence in ALC_FLR and documentation reviews. However, assessment of the developer's arrangements for separating corrections in security flaws from functional corrections is not necessarily an ISO/IEC 17025 testing activity. Limited familiarisation with the extended component and associated methodology is required, with the activity performed or controlled within the ISO/IEC 17065 certification function.

Note: FRU_RSA.1/2 and FDP_RIP.1 are Security Functional Requirements from ISO/IEC 15408-2; existing ASE, ADV, AGD and ALC components are Security Assurance Requirements from ISO/IEC 15408-3; ADV_ARC.2, ADV_PDM.1, AGD_DEC.1, ALC_FLR.4, ALC_SBM.1 and ALC_PSR.1 are proposed extended components from the ENISA study *Cyber Resilience Act implementation via EUCC and its applicable technical elements* (January 2025) and are included solely to identify potentially relevant evaluation activities; complete definitions, dependencies and evaluation methods would be needed before formal use.

The remaining differences must be addressed according to their nature. **Free-of-charge security updates** under Annex I, Part II(8) are a manufacturer obligation assessed on non-technical grounds, rather than a notified-body conformity-assessment activity or an additional CAB competence gap. **Technical update-security** and **vulnerability-handling requirements** remain subject to the applicable assessment. The declared support period is reviewed through the relevant technical documentation and user information. **Compliance with Article 14 operational incident-reporting obligations falls outside** the notified body's assessment of Annex I. **Technical activities** such as code-level exploitation-mitigation assessment and physical fault-injection or tamper testing remain product-, risk-, assurance- and scope-dependent.

Section 7.6 (IT Security Assessment Capability Gap Analysis: CRA and EUCC) sets out the practical implications for an ITSEF that is currently accredited at the 'substantial' level, and the skills-development programme needed to close the identified competence gaps.

2.3 Module B: Conformity Assessment Activity Comparison

Table 3 compares the assessment activities relevant to CRA Module B with their closest methodological counterparts in RED Module B and EUCC. The categories are used solely to structure this analysis and do not constitute a testing taxonomy prescribed by the CRA. Coverage depends on the product, applicable requirements, evaluation boundary and demonstrated CAB competence.

Table 3. Conformity Assessment Activity Comparison, CRA-Module B vs RED-Module B vs EUCC

ACTIVITY	CRA	RED	EUCC
Documentation & design review	Technical-documentation, supporting-evidence and design-adequacy review	Documentation and product-design/concept review	Security Target Evaluation (ASE); Design & Architecture Review (ADV); Guidance Review (AGD); review of the evaluated configuration and, where required, its secure default state.
Functional testing	Functional security testing, as required by the product and risks	Functional testing of applicable access-control, update, network-security, resilience and other mechanisms	Functional Security Testing (ATE)
Configuration inspection	Configuration, settings and secure-default assessment	Configuration and default-state inspection	Review of AGD_PRE preparative-procedure evaluation and AGD_OPE operational guidance, supported by relevant ADV and ATE evidence. CRA secure-default coverage must be demonstrated; proposed ADV_ARC.2 is an analytical extension, not a current EUCC component.
Vulnerability analysis	Vulnerability analysis and necessary security testing	Limited foothold through GEC-1 and mechanism-specific testing	Vulnerability analysis under AVA, with depth depending on the assurance level.
Assessment and testing of cryptographic mechanisms Does not imply a separate cryptographic-validation scheme.	Assessment of cryptographic suitability and implementation, according to product risks and applicable requirements	Assessment of cryptographic suitability, implementation and confidential-key protection under EN 18031 CRY and CCK.	Evaluation of applicable FCS requirements, primarily through the dedicated Cryptographic Analysis technique (algorithm/protocol conformance per ISO/IEC 18367, entropy analysis per ISO/IEC 20543, protocol verification per ISO/IEC 29128-1), supported by ATE functional testing, AVA vulnerability/attack-resistance analysis and, where relevant, ADV implementation evidence.
Physical & hardware testing	Applicable to products and risks requiring physical or hardware-security assessment	Limited coverage through boot integrity in Part 3 and hardware-backed storage mechanisms	ATE and AVA activities applied to hardware TOEs, subject to the ITSEF's accredited technology scope, evaluation techniques and applicable attack potential.
Code & binary analysis	May be required for selected products and evaluation methods	**Not prescribed as a standalone assessment activity**	Partially covered through the Source Code Review evaluation technique (Annex A.2.1) and, where applicable, ADV_IMP implementation-representation assessment, supported by AVA vulnerability analysis and

ACTIVITY	CRA	RED	EUCC
			penetration testing (Annex A.2.3, including ISO/IEC 20004-based methods). Coverage depends on the ITSEF's accredited scope and the applicable assurance level. EUCC does not expressly require binary-hardening or exploitation-mitigation verification as standalone activities, while SBOM-driven dependency analysis has no direct current EUCC equivalent.
Process & lifecycle assessment	Review of development evidence relevant to Annex I, Part I and assessment of Annex I, Part II vulnerability-handling processes	**No equivalent process-level assessment**	Partial coverage through applicable ALC lifecycle-support components, including ALC_FLR, and EUCC vulnerability-management provisions.
Vulnerability handling examination	Examination of the manufacturer's Annex I, Part II vulnerability-handling processes	**No equivalent process-level assessment**	Partial foundation through ALC_FLR (flaw-remediation evaluation), and EUCC vulnerability-management and disclosure provisions (Regulation (EU) 2024/482, Chapter VI).
Compliance mapping	Tracing applicable CRA essential requirements to evidence and conclusions; identifying gaps in coverage.	Tracing applicable RED essential requirements to evidence and conclusions; identifying gaps in coverage.	Tracing ST/PP requirements and assurance criteria to ITSEF findings; CB review for the certification decision.

The comparison shows that RED does not prescribe standalone activities equivalent to CRA-oriented **code and binary analysis**, **manufacturer process and lifecycle assessment**, or the **examination of vulnerability-handling processes**. Some adjacent RED competence may nevertheless provide a limited foundation, particularly for product-level security-mechanism testing.

RED Module B is predominantly a point-in-time, product-focused assessment, examining the equipment and its implemented security mechanisms. **CRA Module B extends the assessment to the adequacy of the product's technical design and development and to the manufacturer's vulnerability-handling processes**, addressing how security is maintained throughout the support period as well as how the product performs at the time of assessment.

EUCC offers broader methodological alignment but not automatic equivalence. The remaining gaps depend on the ITSEF's accredited scope, assurance level, technology coverage, evaluation methods and demonstrated personnel competence. EUCC CB and ITSEF capabilities must also be considered together because the certification-decision and technical-evaluation roles are separated.

2.4 From RED to CRA-Module H

Of the four CAB transition paths assessed in this study, this is the smallest gap. RED notified bodies accredited under ISO/IEC 17021-1 have an established foundation of management-system certification relevant to CRA Module H. However, they must adapt their certification system, procedures, documentation and competence arrangements to the CRA context and extend their scope of accreditation and notification accordingly. RED accreditation does not automatically demonstrate compliance with CRA Module H. The remaining **gap is limited to two areas**.

1. **Development and vulnerability-handling controls within the quality system.** This capability is specific to CRA and has no RED equivalent. Additional competence concerns the arrangements required by CRA Annex VIII, Part IV, points 3.2–3.3 and 4, supporting Annex I, Parts I and II. The assessment does not require the manufacturer to operate a particular SDLC framework.

2. **Product-specific assessment of quality-system design controls.** Both frameworks require this competence: CRA in Annex I, Part I; RED in Article 3(3)(d), (e) and (f), supported where applicable by EN 18031:2024.

Section 9.4 (RED – CRA Module H Gap Analysis and Competence Comparison) sets out the full comparative analysis.

3 Scope and Approach

The analysis covers the two CRA conformity assessment procedures that require a notified body.

- **CRA-Module B** (EU-type examination) compared with **RED-Module B** (the essential requirements of Article 3(3), points (d), (e), and (f), of Directive 2014/53/EU) and **EUCC** (established by Commission Implementing Regulation (EU) 2024/482). Within the EUCC comparison, certification bodies accredited under ISO/IEC 17065 and ITSEFs accredited under ISO/IEC 17025 are considered as separate transition paths.
- **CRA-Module H** (full quality assurance) compared with **RED-Module H** (the same RED Article 3(3)(d)(e)(f) essential requirements, assessed via ISO/IEC 17021-1 rather than ISO/IEC 17065). EUCC has no Module H equivalent, so this comparison is against RED-only.

The document uses three categories of requirements to structure the analysis.

1. **The range of products (product category / family in scope) to which the assessment activities apply**, since each product category requires the specific technical competences needed to prove compliance with the applicable cybersecurity requirements. The document focuses on the elements included in the scope of accreditation for notification (by a NAB) or scope of notification (by an NA) and analyses the CAB's technical competence against them.
2. **The type of conformity assessment activity** (testing, audits etc) carried out by the CAB. **This is the core of the analysis**, since it determines the technical competences that a notified CAB must hold. These requirements also depend on the product conformity strategy the manufacturer chooses (the NLF module), which points to a preferred harmonised accreditation standard. RED and EUCC each have a well-defined set of competences here, because both have an applicable harmonised (RED) or cited (EUCC) product standard. The CRA's harmonised product standards have not yet reached maturity; the document therefore sets out a set of commonly agreed technical competences expected to satisfy the requirements once the final standards are cited.
3. **The statutory, organisational, and procedural requirements** that a notified CAB must meet as a condition of notification and continued operation. These cover competence, impartiality, independence and reliability. These requirements are substantively harmonised across all three frameworks. CRA and RED both follow the EU's New Legislative Framework (NLF) model and EUCC layers its own requirements on top of the same accreditation regulation.

The first two categories are where the real gaps sit and are the focus of this document.

LIST OF ABBREVIATIONS	
ADV	Development in the context of EUCC and CRA
AGD	Guidance documents in the context of EUCC and CRA
ALC	Life-cycle support in the context of EUCC and CRA
ASE	Security Target evaluation in the context of EUCC and CRA
ATE	Tests in the context of EUCC and CRA
AVA	Vulnerability assessment in the context of EUCC and CRA
BSI	Germany's Federal Office for Information Security
CAB	Conformity Assessment Body
CB	Certification Body
CC	Common Criteria (ISO/IEC 15408)

CD	Continuous Development
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CI	Continuous Integration
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CVD	Coordinated Vulnerability Disclosure
EAL	Evaluation Assurance Level
ESR	Essential Security Requirement
EUCC	European Common Criteria-based cybersecurity certification scheme
FCS	Cryptographic Support in the context of EUCC and CRA
FLR	Flaw remediation in the context of EUCC and CRA
HS	Harmonised standard(s)
ISMS	Information security management system
ISO	International Organization for Standardization
ITSEF	IT Security Evaluation Facility
NA	Notifying Authority
NAB	National Accreditation Body
NB / NoBo	Notified body
NCCA	National Cybersecurity Certification Authority
NLF	New Legislative Framework
PP	Protection Profile
RED	Radio Equipment Directive
SAR	Security Assurance Requirement in the context of EUCC and CRA
SBOM	Software Bill of Materials
SDLC	Software Development Lifecycle
SotA	State of the Art document
ST	Security Target in the context of EUCC and CRA
TMB	Technical Management Board, in the ISO context
TOE	Target of Evaluation (Common Criteria)
VM	Vulnerability management in the context of EUCC and CRA

4 Notification Requirements and Their Accreditation Basis

CRA Art. 39 and RED Art. 26 – both titled 'Requirements relating to notified bodies', reflecting the NLF template in Decision 768/2008/EC, Annex II – **set out the conditions** a CAB must satisfy for notification, including legal status, independence, impartiality, organisational structure and freedom from conflicts of interest, personnel competence, liability, confidentiality and participation in standardisation and coordination activities. Subcontracting and the use of subsidiaries is addressed separately, in CRA Art. 41 and RED Art. 28, which require any subcontractor or subsidiary to itself meet the respective Arts. 39 and 26 requirements. They form an integrated set of conditions and should not be treated as separate organisational 'eligibility' requirements outside accreditation and technical-competence requirements within accreditation.

EUCC's equivalent is layered. CSA Art. 60(1) and its Annex set the base accreditation requirement. IR (EU) 2024/482 Ch. IV then adds EUCC-specific layers. Art. 20a specifies accreditation requirements. Arts. 21–22 add requirements for certification bodies and ITSEFs (including for certification bodies, criteria for assurance level 'high') and Arts. 23–24 govern notification. Monitoring is separate (Arts. 25–26).

Under Article 2(10) of Regulation (EC) No 765/2008, accreditation attests that a conformity assessment body meets the requirements set by the harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity-assessment activity.

Accreditation therefore addresses the CAB's overall competence and capability, including the applicable organisational, impartiality, management-system, resource, process and technical requirements. Although Recital 12 describes accreditation as the *preferred means of demonstrating the technical competence of those bodies*, this does not limit accreditation to technical matters. The notifying authority remains responsible for the notification decision and must verify that the scope of the accreditation and any supplementary evidence cover all requirements of the applicable legislation and requested scope of the notification.

Existing evidence concerning impartiality, independence, confidentiality, liability, governance, subcontracting and certification processes should be considered where its continuing validity and applicability to the requested CRA scope are demonstrated. Additional assessment should focus on CRA-specific requirements and matters not adequately covered by that evidence. This approach supports efficient assessment while preserving verification of all applicable notification requirements.

Table 4. Notification and Accreditation Basis, by Framework and Module

REQUIREMENT	CRA	RED	EUCC
Legal basis for accreditation	Reg. (EU) 2024/2847, Art. 39–40, ref. to Reg. (EC) 765/2008	Dir. 2014/53/EU, Art. 26–27, ref. to Reg. (EC) 765/2008	IR (EU) 2024/482, Arts. 20–26, ref. to CSA Art. 60 and Reg. (EC) 765/2008
Accreditation standard(s) Module B	EN ISO/IEC 17065 + testing and inspection capability required	EN ISO/IEC 17065, supplemented by the applicable ISO/IEC	ISO/IEC 17065 (CB) + ISO/IEC 17025 (ITSEF)[9]

[9] According to European Accreditation (EA). EA-INF/17: 2026: Register of EA resolutions for use by EA, National Accreditation Bodies and EA evaluators, Rev. 16. TMB Resolution 2022 (09) 01, '[…] the best suitable standard for the accreditation of bodies performing evaluation/on-site audits and surveillance as described in the EUCC scheme would be ISO/IEC 17065. But considering that these activities are performed for many years by ITSEFs (laboratories) and that has been accepted in Mutual Recognition Arrangements (CCRA and SOGIS-MRA) and by all parties involved, the TMB accepts the application of these activities under ISO/IEC 17025. But ENISA is asked to transition those activities, which do not fit under ISO/IEC 17025, to

REQUIREMENT	CRA	RED	EUCC
		17025 competence requirements where testing is undertaken	
Accreditation standard(s) Module H	EN ISO/IEC 17021-1	EN ISO/IEC 17021-1	No formal equivalent[10]
Role of NAB	Assesses the CAB against the applicable harmonised accreditation standard and relevant CRA requirements, covering organisational arrangements, impartiality, resources, processes and technical competence. The accreditation certificate and scope support notification.	Assesses the CAB against the applicable harmonised accreditation standard and relevant RED requirements, covering organisational arrangements, impartiality, resources, processes and technical competence. The accreditation certificate and scope support notification.	Accredits CBs and ITSEFs against the applicable accreditation standards and EUCC-specific requirements, covering their respective organisational, process and technical competences. Accreditation is mandatory; additional authorisation applies for assurance level 'high'.
Alternative to accreditation	Yes – Art. 42(3): documentary evidence to notifying authority	Yes – Art. 29(3): documentary evidence to notifying authority	No – accreditation is mandatory; authorisation is additionally required for 'high'.
Oversight authority	Notifying authority (national)	Notifying authority (national)	**The National cybersecurity certification authority (NCCA[11])** supervises CBs and ITSEFs, notifies them to the Commission, and authorises their activities at assurance level 'high' (CSA Articles 58(7), 60(3) and 61; EUCC Articles 21–25).

certification bodies which shall be accredited according to ISO/IEC 17065. The recommended transition period is 5 years'. Available from: http://www.european-accreditation.org/ FAQ '48.1 Question on Choice appropriate standard for accreditation. (ISO/IEC17025 or ISO/IEC 17020)'.

[10] Pilots on the EUCC-CRA mapping indicate that site audits performed under the EUCC state-of-the-art *Minimum Site Security Requirements* v2, Feb 2025, may cover part of a Module H quality-system assessment. Such audits are carried out by bodies accredited under ISO/IEC 17025 (ITSEFs) and ISO/IEC 17065 (CBs). This is a pilot experience, not a recognised formal equivalence.

[11] NCCAs are subject to peer review under CSA Article 59, with outcomes examined by the ECCG. ENISA may participate in peer review; it is not the supervisory authority for EUCC CABs.

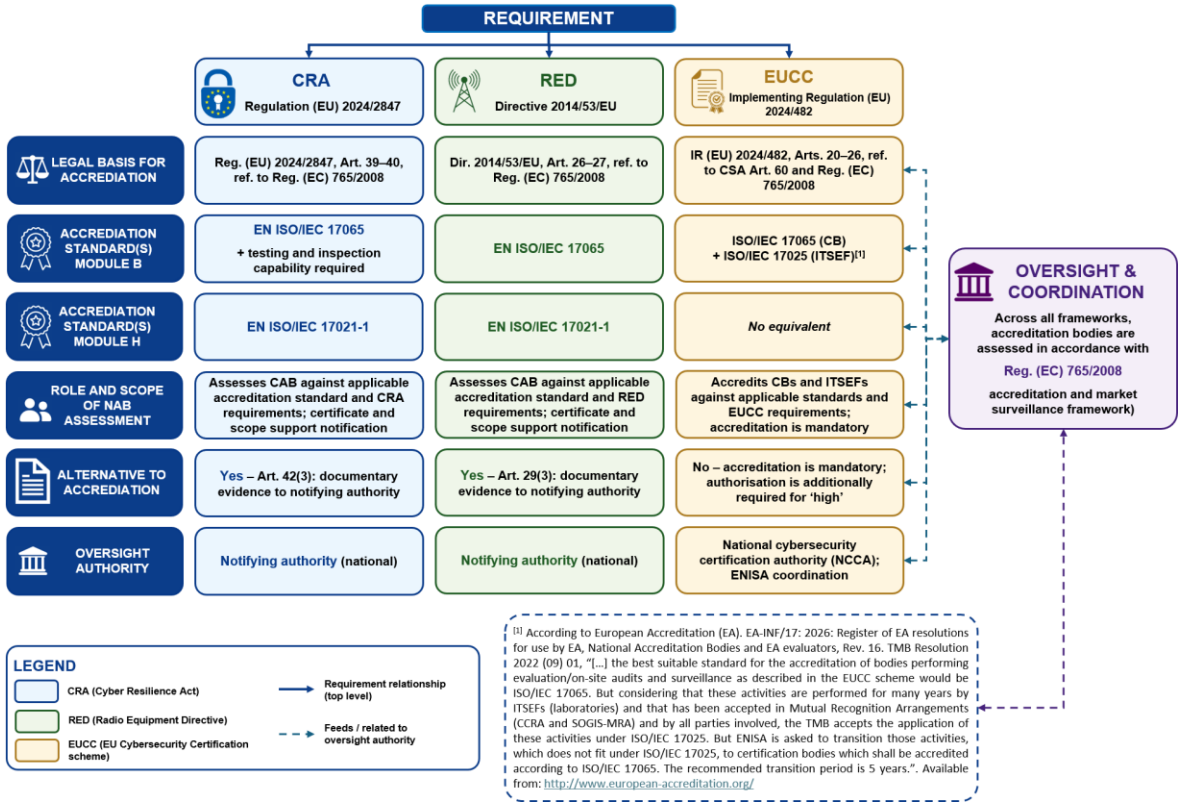


Figure 1. Notification and Accreditation Basis, by Framework and Module

Note on the accreditation baseline. The EA Accreditation for Notification (AfN) Project Report[12] (May 2026, Annex C), identifies **EN ISO/IEC 17065** as the preferred accreditation standard for EU-type examination **under both CRA Annex VIII, Part II and RED Annex III**. **For CRA Module B**, the report additionally specifies that **testing and inspection capabilities are required**. The detailed accreditation bases for CRA and RED Module B are addressed in Sections 5.2 and 6.2, respectively.

Under EA-2/17 M:2026, Supplement 1, Table 1, **CRA Module B** (Annex VIII, Part II) is accredited against EN ISO/IEC 17065 (the obligatory harmonised standard) with obligatory requirements for:

- conformity judgement and certification decisions (***cd***), citing the applicable EN ISO/IEC 17065:2012, clauses 4.1.2, 4.1.3, 7.5 and 7.6;
- product-related professional judgement (***pk***), citing EN ISO/IEC 17020:2012, clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10;
- testing where required (***t***), citing the applicable EN ISO/IEC 17025:2017 clauses 6 and 7, excluding 7.9.

These are competence requirements within the accreditation approach, not a requirement to hold three separate accreditations. The transition arrangements are noted in Section 1.2.

[12] European Accreditation. *EA Accreditation for Notification (AfN) Project – Report Updated May 2026*. Brussels: EA, 2026. Available from: https://european-accreditation.org/wp-content/uploads/2025/10/AFN-Project-May-2026.pdf.

The organisational eligibility criteria (including legal personality, independence, impartiality, liability arrangements, confidentiality and control of subcontracting) **are substantially aligned under CRA Article 39 and RED Article 26**, as both follow the New Legislative Framework model. **EUCC structures these safeguards differently** through the CSA accreditation framework, the EUCC Regulation, EN ISO/IEC 17065 for CBs, EN ISO/IEC 17025 for ITSEFs and the applicable state-of-the-art accreditation documents. It **distinguishes between two types of CAB: CBs and ITSEFs**.

This structural similarity may allow a RED notified body to reuse relevant organisational and certification-system evidence when applying for CRA notification. However, the CRA notifying authority must still verify compliance with Article 39 and competence in the requested CRA scope. RED notification does not confer automatic eligibility under the CRA.

Similarly, **an EUCC CB accredited against EN ISO/IEC 17065 may reuse relevant organisational and certification-system evidence.** However, it must reassess that evidence in the CRA context and demonstrate compliance with CRA Article 39 and competence to perform the complete CRA Module B procedure within the requested notification scope, including evaluation, review, decision-making, certification and control of any subcontracted activities.

An EUCC ITSEF accredited only against EN ISO/IEC 17025 cannot rely on that accreditation alone to qualify as a CRA Module B notified body. Its accreditation demonstrates competence to perform testing and evaluation activities, but not the certification and decision-making architecture required to control the complete conformity-assessment procedure and issue EU-type examination certificates. An ITSEF could however support a CRA notified body as a controlled subcontractor. Alternatively, it may seek CRA notification after establishing the necessary certification-body architecture, obtaining the applicable expanded accreditation and demonstrating compliance with the CRA requirements.

CAB competence is assessed against the applicable accreditation and notified-body requirements for the requested conformity assessment procedure and product scope. Relevant harmonised standards, common specifications adopted under Article 27, and other European or international standards and technical specifications support the technical knowledge, methods and evidence needed for that scope. Their legal effects differ. Harmonised standards and adopted common specifications provide a presumption of conformity only for the requirements they cover. Other standards may support the assessment of technical solutions but do not, by themselves, provide such a presumption. Where coverage is absent or incomplete, the CAB must demonstrate the competence to assess the manufacturer's solutions directly against the relevant CRA essential requirements.

The table below covers only the CAB-facing notification criteria – what a body itself must demonstrate to be notified. It does not cover the NA's own obligations (competence, independence from the CABs it notifies) or the procedural act of notification (informing the Commission and other Member States, maintaining the notified-body listing, monitoring and withdrawal) – these fall outside the scope of this analysis, which is limited to CAB competence and eligibility.

Table 5. Notification Requirements for Module B

REQUIREMENT	CRA	RED	EUCC
Independence and impartiality	Art. 39(3) – (4): third-party independence; no design/manufacture involvement	Art. 26(2) – (6) and (8): substantially equivalent to NLF requirements	ISO/IEC 17065:2012, clause 4.2; ENISA EUCC SotA *Accreditation of CBs for the EUCC Scheme*[13], section 7.2.3: separation of evaluation and certification functions, with organisational and

[13] EUCC Scheme, State-of-the-Art Document, Accreditation of CBs for the EUCC scheme, Version 1.6b, November 2024, available from https://certification.enisa.europa.eu/publications/

REQUIREMENT	CRA	RED	EUCC
			personnel safeguards where the CB and ITSEF share a legal entity.
Organisational structure	NLF-standard covers top-management commitment and documented procedures.	Art. 26(5) – (7) is substantially equivalent to NLF requirements.	ISO/IEC 17065 + ISO/IEC 17025 requirements; ENISA SotA specifies CB/ITSEF interface requirements.
Liability / insurance	Art. 39(9) requires liability insurance or state liability	Art. 26(9) is substantially equivalent to NLF requirements	CSA Art. 60 Annex: adequate financial resources and national requirements apply[14].
Subcontracting	Art. 41: permitted with oversight; subcontractor meets same requirements.	Art. 26(5) and Art. 28 are substantially equivalent requirements; the notified body remains fully responsible.	ITSEF as subcontractor to CB: formal selection, approval, monitoring; subcontracted ITSEF subject to accreditation.
Confidentiality	Art. 39(10): covers professional secrecy and protection of proprietary rights.	Art. 26(10) is substantially equivalent to the NLF requirement.	EUCC Arts. 21–22: enhanced confidentiality for 'high' assurance; technical/operational measures for sensitive information.

[14] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) – Annex, Requirements to be met by conformity assessment bodies.

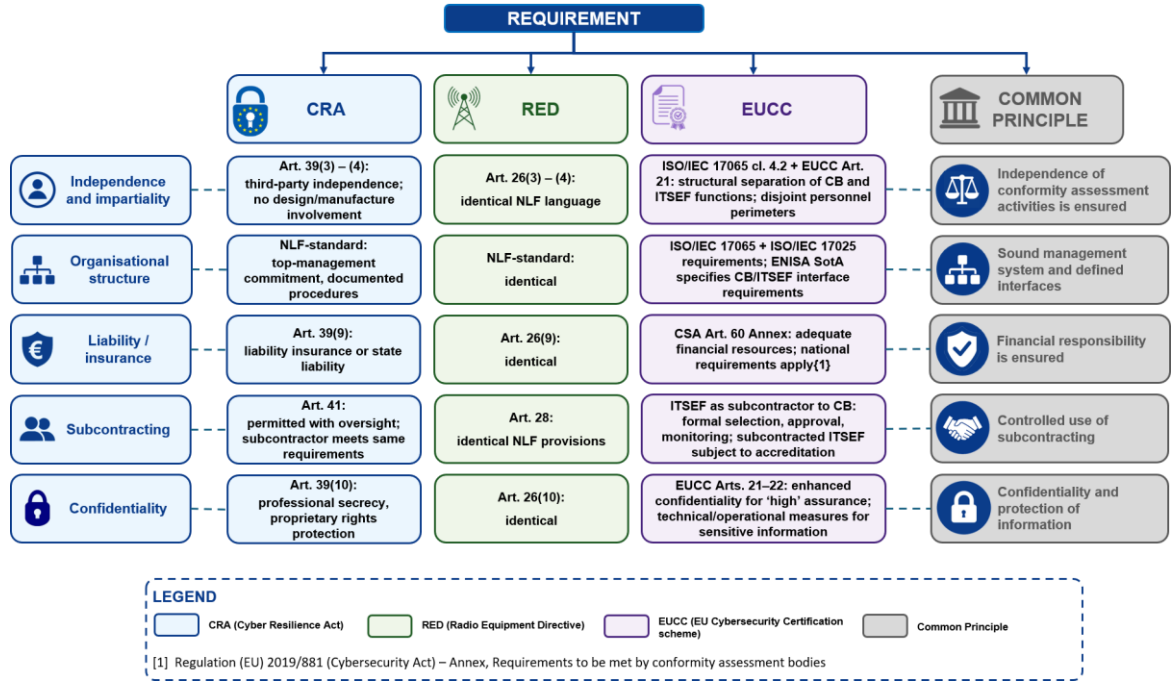


Figure 2. Notification Requirements for Module B

5 CRA-Module B: CAB Technical Competences

5.1 Scope Of Accreditation

According to EA-2/17 M: 2026, the main elements to be included in the scope of accreditation are:

a. **The harmonised standard (HS) used as the accreditation reference and applied in full** – here EN ISO/IEC 17065.
b. **The applicable legislation** – Regulation (EU) 2024/2847, including the essential cybersecurity requirements in Annex I, Parts I and II, the notified-body requirements in Article 39, and the Module B conformity-assessment procedure in Annex VIII, Part II.
c. **The conformity assessment procedure**– Annex VIII, Part II, Module B: EU-type examination.
d. **The product categories or families covered** – identified with sufficient precision. The scope may cover the important products in Annex III (Classes I and II), the critical products in Annex IV, and other products with digital elements. Module B is not limited to the Annex III and IV categories; manufacturers of other products may also choose Module B+C under Article 32(1), subject to the CAB's demonstrated competence and notification scope.
e. **The applicable product characteristics or specifications** – including the relevant CRA essential cybersecurity requirements, harmonised product standards, common specifications or other applicable sectoral and technical documents.

The scope of accreditation should be sufficiently granular to support the requested notification scope. Under CRA Article 42(2), the application must describe the conformity-assessment activities, procedures or modules and the product or products with digital elements concerned and, where available, include an accreditation certificate attesting compliance with Article 39. Article 43(3) requires the notification to provide corresponding scope details and an attestation of competence. Once a CRA-specific product classification is established in NANDO, the accreditation scope should be capable of being mapped to that classification. Where notification is not based on accreditation, the evidence provided under Articles 42(3) and 43(4) should contain sufficient scope-specific detail to demonstrate and monitor competence for the requested notification scope.

The role of harmonised standards, common specifications and other technical standards in demonstrating competence for the requested scope is explained in Section 4 (before Table 5).

A CAB notified for CRA Module B must demonstrate the capability to:

1. **assess the adequacy of the technical design and development of products with digital elements**, based on the relevant technical documentation, supporting evidence and representative specimens;
2. **assess conformity with the applicable essential cybersecurity requirements in Annex I, Part I**, including the ability to perform, or have performed, the necessary examinations and tests;
3. **examine the manufacturer's vulnerability-handling processes against Annex I, Part II**, including conducting the periodic audits required by Annex VIII, Part II, to verify that those processes are adequately implemented;
4. **perform these activities through an independent, impartial and consistently controlled conformity-assessment process**.

5.2 Standards for Accreditation for Notification

According to the EA Accreditation for Notification (AfN) Project Report (May 2026, Annex C), accreditation for CRA Annex VIII, Part II is based on **EN ISO/IEC 17065, supplemented by the**

necessary testing and inspection capability. EA identifies EN ISO/IEC 17065 as the best-fit standard because it covers the complete certification activity and links to other relevant conformity-assessment standards through Clause 6.2. EA-2/17 S1 M:2026 now expressly lists CRA Module B under EN ISO/IEC 17065 with *cd+pk+t* requirements, subject to the transition described in Section 1.2.

Directive / Regulation	Regulation (EU) 2024/2847 – Cyber Resilience Act	
Attestation Module / System	Preferred Standard	Justification
Annex VIII, Part II EU-type examination (based on module B)	EN ISO/IEC 17065 + testing and inspection capability will be required	EN ISO/IEC 17065 is considered to be the best fit for this activity and links to other relevant Conformity Assessment Standards through clause 6.2. Note: The periodic audits of the vulnerability handling processes used by the manufacturer is considered also covered by EN ISO /IEC 17065 without specific EN ISO/IEC 17021-1 competence.
Annex VIII, Part IV Conformity based on full quality assurance (based on module H)	EN ISO/IEC 17021-1 + Auditor competence must include specific product knowledge	This module is based on Quality Assurance auditing.

Figure 3. Annex C – EA Accreditation for Notification (AfN) Project Report

Accordingly:

- **ISO/IEC 17065** is the overarching accreditation standard governing the CAB's operation, competence, impartiality, evaluation, review and certification decision;
- **ISO/IEC 17025** provides the relevant competence requirements where testing activities are performed or controlled through EN ISO/IEC 17065 Clause 6.2;
- **ISO/IEC 17020** provides the relevant requirements where inspection activities are performed or controlled through EN ISO/IEC 17065 Clause 6.2.

5.3 Competence Requirements for CRA-Module B Notified Bodies

The tables below list the competence requirements for CRA-Module B Notified Bodies, organised by the three requirement categories introduced in Section 3. Section 5.4 details the competence requirements related to the type of conformity assessment activity.

Table 6. CRA-Module B: Specific requirements related to the scope of accreditation

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCES
Product-specific conformity assessment capability	Capability to assess the adequacy of the technical design and development of the product, specific to the product category/family in scope	CRA – Annexes III and IV; Art. 39(7); EA-2/17 S1 M:2026, citing EN ISO/IEC 17020:2012, clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10.

Table 7. CRA-Module B: Specific requirements related to the type of conformity assessment activity

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCES
Competence to perform or control IT-security testing	Functional security testing includes Configuration and Settings Inspection; Vulnerability Analysis; Assessment and testing of cryptographic mechanisms, where applicable; Physical and Hardware Security Testing, where applicable; Code and Binary Analysis, where applicable.	CRA Annex I, Part I; Annex VIII, Part II, points 4.2 – 4.5; Article 39(6) – (7); EN ISO/IEC 17065:2012, Clause 6.2; relevant requirements of ISO/IEC 17025:2017.
Competence to examine technical design and documentation	Documentation and Design Review	CRA Annex VII; Annex VIII, Part II, points 1 – 4; Article 39(6) – (7); EN ISO/IEC 17065:2012. ENISA Draft Document on Personnel Competences for NoBos.
Competence to execute testing activities in a competent, independent, and reproducible manner	The abilities required are Method Verification and Validation; Assurance of result validity; Traceability; Measurement Uncertainty; Management of deviations and nonconformities; Operational and Information Control.	ISO/IEC 17025:2017, Clauses 4.1 – 4.2, 6.1 – 6.6, 7.1 – 7.8 and 7.10 – 7.11, as applicable through EN ISO/IEC 17065:2012, Clause 6.2
Competence to assess vulnerability-handling processes put in place by the manufacturer	The abilities required are Process and Lifecycle Assessment; Vulnerability Handling and Reporting Process Assessment; Knowledge required of the technology used to operate the process; the way the process is operated; defects, failures, or deficiencies that may occur during operation; and the ability to understand the significance of deviations found against normal intended use.	CRA Annex I, Part II; Annex VIII, Part II, points 1, 4.1, 7 and 8; Article 39(6) – (7); EN ISO/IEC 17065:2012; EA-2/17 S1 M:2026, requirement '*pk*', referencing EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; ISO/IEC 30111:2019 (vulnerability handling processes); ISO/IEC 29147:2018 (vulnerability disclosure)
Competence to evaluate and document conformity evidence	Ability to undertake Compliance Mapping and Evidence Aggregation	CRA Annex VII; Annex VIII, Part II, points 3 – 6; Article 39(7); EN ISO/IEC 17065:2012, Clauses 7.4 – 7.6
Outsourced capabilities	Subcontracting requirements as per the standard	CRA Articles 39(6) and 41; EN ISO/IEC 17065:2012, Clauses 6.2.2 and 7.5 – 7.6; ISO/IEC 17025:2017, Clause 6.6, where applicable

Table 8. CRA-Module B: Structural and process requirements

REQUIREMENT CATEGORY	REQUIREMENTS	STANDARD REFERENCES
General requirements	Legal and contractual matters; management of impartiality; liability and financing; non-discriminatory conditions; confidentiality; publicly available information	ISO/IEC 17065:2012, clause 4
Structural requirements	Organisational structure and top management; mechanism for safeguarding impartiality	ISO/IEC 17065:2012, clause 5
Process requirements	Application, application review, evaluation, review, certification decision, certification documentation, directory of certified products, surveillance, changes affecting certification, termination/reduction/suspension/withdrawal of certification, records, complaints and appeals	ISO/IEC 17065:2012, clause 7
Management system requirements	**Option A** (standalone management system): general documentation, control of documents, control of records, management review, internal audit, corrective actions, preventive actions. **Option B**: a management system compliant with ISO 9001:2015, which does not additionally require ISO 9001 certification of the management system	ISO/IEC 17065:2012, clauses 8.2–8.8; ISO 9001:2015

5.4 Competence Requirements by Conformity Assessment Activity

This section sets out the testing and evaluation activities that define the technical competence required of a CRA notified body (NB) performing conformity assessment under CRA Module B (EU-type examination). The activities derive from the CRA essential cybersecurity requirements (Annex I, Parts I and II), the manufacturer obligations in Article 13, and the Module B examination procedure in Annex VIII, Part II.

Determination methods. A CRA notified body determines conformity by:

1. **examining the technical documentation** and **supporting evidence**, to assess the adequacy of the technical design and development of the product against the essential cybersecurity requirements;
2. **examining the process documentation** and **supporting evidence** for the manufacturer's **vulnerability-handling processes**;
3. **verifying that specimens** are developed or manufactured in conformity with the technical documentation;
4. **carrying out** – or arranging for – **appropriate examinations and tests**, to check that either (a) the relevant harmonised standards have been applied or (b) the manufacturer's solutions meet the corresponding essential cybersecurity requirements.

5.4.1 Documentation and Design Review

Review and analysis of manufacturer-provided documentation, to verify that essential cybersecurity requirements are properly designed, implemented, documented and maintained, and that the specimens conform to the technical documentation.

- **Security architecture review.** Examination of security-architecture documents, threat models, and design decisions, to verify implementation of secure-by-design principles throughout the product lifecycle.

- **Review of risk assessment documentation.** Review of the risk assessment for soundness and completeness, examining whether all risk factors relevant to the product's intended purpose, reasonably foreseeable use, and conditions of use have been identified, maintained and documented.

  NOTE: The manufacturer must assess and document which risk factors apply to the product. Two categories of violation result in non-compliance: (i) *undeclared* risk factors – factors defined in clauses 4.8.2.1–4.8.2.5 that apply to the product but are not identified in the risk factor assessment; and (ii) *misdeclared* risk factors – an incorrect identification of which risk factors apply.
- **User documentation review.** Assessment of user-facing information, including security guidance, default-settings documentation and end-of-support communication.
- **User and integrator documentation review.** Assessment of information needed to install, configure, integrate, use and decommission the product securely, including security assumptions, default settings, update instructions, the vulnerability contact point, the coordinated vulnerability disclosure policy and support-period information (CRA Annex II). For products intended for integration into other products with digital elements, the review also covers the information necessary for the integrator to comply with the Annex I essential cybersecurity requirements and Annex VII documentation requirements (Annex II, point 8(f)).
- **Technical documentation review**. Review of technical documentation describing the product's design and development solutions and evidence supporting conformity. Development records may be relevant supporting evidence; the existence of an SDLC is not an assessment criterion.
- **Policy documentation review.** Review of security policies, access-control policies, isolation policies and exception-handling procedures.

5.4.2 Functional Security Testing

Functional security testing is the active testing of security mechanisms to verify that they function as specified under normal and boundary conditions. They include the following tests.

- **Access control testing.** Authentication, authorisation enforcement, role-based access, privilege separation, credential management.
- **Isolation mechanism testing.** Process isolation, origin isolation, domain sandboxing, container isolation, VM separation, network segmentation.
- **Cryptographic function testing.** TLS/SSL implementation, certificate handling, cipher suites, key management, encryption at rest and in transit.
- **Update mechanism testing.** Automatic update delivery, signature verification, emergency update capability, delta updates.
- **Boot integrity testing.** Secure boot chain, measured boot, component integrity verification, chain-of-trust establishment.
- **Logging and audit testing.** Security event logging, log integrity, log access controls, audit-trail completeness.
- **Input validation testing.** Input sanitisation, parser security, protocol handler security, content filtering.

  NOTE: ETSI EN 304 626 for operating systems, ETSI EN 304 625 for network interfaces and ETSI EN 304 620-1 for virtual private networks, include MI-BTIN (boundary testing of inputs that may cause memory errors), under the secure-software-design-and-development requirement TR-SSDD. Its applicability depends on the security profile defined in the relevant vertical standard.
- **Default security settings verification.** Confirmation that products ship with secure default configurations (no default passwords, minimal exposed interfaces).

  NOTE: TR-SDEF and MI-ADEF concern secure-by-default configuration and authorisation by default for access to security-relevant assets. They appear, among others, in draft ETSI EN 304 626 for operating systems and ETSI EN 304 625 for

network interfaces. Their applicability depends on the security profile defined in the relevant standard.

- **Rollback protection testing.** Where the product's security profile warrants it, attempting version rollback via standard and forced methods, and verifying prevention or detection at boot/runtime.
  NOTE: Not all vertical standards require rollback protection; applicability depends on the product's security profile.
- **Enterprise policy configuration.** Verification that enterprise deployment configurations (group policies, MDM) correctly enforce security settings.

5.4.3 Configuration and Settings Inspection

Examination and verification of product configuration settings, security policies and deployment parameters to ensure they meet security requirements.

- **Configuration file inspection.** Review of boot configuration files, security policy settings, certificate stores, key databases and system configuration.
- **Default settings audit.** Systematic verification that all default configuration values meet security requirements (no default passwords, minimal permissions).
- **Extension/plugin security review.** Assessment of extension permission models, sandboxing, manifest validation, API access controls and sideloading restrictions.
- **Network configuration testing.** Inspection of firewall rules, network segmentation, interface configurations and management plane separation.
- **Debug interface configuration.** Verification that debug and management interfaces (JTAG, serial console, network management) are properly secured or disabled.
  NOTE: The vertical standards define MI-PDDI-1 (document protection), MI-PDDI-2 (physical access), MI-PDDI-3 (local software access), and MI-PDDI-4 (network access) as separate mitigations depending on the security profile.
- **Enterprise policy configuration.** Verification that enterprise deployment configurations (group policies, MDM) correctly enforce security settings.

5.4.4 Vulnerability Analysis

Activities ranging from identification of known vulnerabilities to adversarial testing for exploitable vulnerabilities through simulated attacks, using both automated and manual techniques.

- **Known vulnerability scanning.** Verification that the product contains no known exploitable vulnerabilities (CVE checking against the SBOM, dependency scanning).
  NOTE: EN 304 626 includes the MI-KEVT and MI-SCAN vulnerability-testing and scanning mitigations, requiring current tools and cross-checking against the manufacturer's documented vulnerability list.
- **Attack resistance testing.** Resistance to known attack techniques such as fuzzing, fault injection, timing attacks, buffer overflow and bypass attempts.
- **Penetration testing.** Structured security assessment by internal or external teams to find exploitable vulnerabilities.
- **TOCTOU analysis.** Review of time-of-check-to-time-of-use windows, including dynamic analysis and exploitation attempts where feasible.
- **Fuzzing.** Automated generation of malformed or random inputs, to discover crashes, hangs and security flaws in parsers, protocols and interfaces.
  NOTE: MI-FZ95, the instrumented-runtime-testing mitigation included in draft ETSI EN 304 620 for virtual private networks, ETSI EN 304 625 for network interfaces and ETSI EN 304 626 for operating systems, requires instrumented execution reaching at least 95% code coverage with the detection of runtime memory-access errors.

- **Bypass attempt validation.** Attempts to circumvent security controls (e.g. disabling secure boot, bypassing authentication, escalating privileges).
- **Component modification detection.** Modifying boot components or system files, to verify that tampering is detected and blocked.
- **Network traffic analysis.** Capture and analysis of network communications, to verify encryption, detect data leaks and validate protocol compliance.

5.4.5 Assessment and testing of cryptographic mechanisms

Specialised testing of cryptographic implementations, protocol compliance, key management and certificate handling to ensure data protection requirements are met.

- **TLS/SSL protocol compliance.** Testing TLS version support against applicable EUCC/ENISA state-of-the-art documents and recognised European, national or international cryptographic catalogues, including BSI, NIST and ETSI references where relevant, together with cipher-suite restrictions, downgrade protection and perfect forward secrecy.
- **Certificate validation testing.** Certificate chain validation, revocation checking (OCSP/CRL), Certificate Transparency and pinning.
- **Key management assessment.** Cryptographic key generation, storage, rotation, isolation and destruction practices.
- **Random number generation testing.** Verification that cryptographic random number generators meet security requirements.
- **VPN tunnel security testing.** VPN protocol implementation, tunnel integrity, authentication and data confidentiality mechanisms.
- **Data-at-rest encryption testing.** Storage encryption for sensitive data, credentials, keys and user information.
- **Hardware-backed crypto verification.** Integration with hardware security modules (HSM, TPM) for cryptographic operations.

5.4.6 Physical and Hardware Security Testing

Testing that requires physical access to hardware or specialised equipment, particularly relevant for boot managers, IoT devices and embedded systems.

NOTE: This competence category is not relevant for software-only products.

- **Hardware platform testing.** Product behaviour across different hardware architectures and platform configurations.
- **Debug interface testing.** Verification that debug ports (JTAG, serial console) are properly secured or disabled in production.
  NOTE: The vertical standards define MI-PDDI-2 (protect or disable physical access to debug and management interfaces) as required for security profiles involving exposure to physical threats.
- **Fault injection testing.** Physical fault injection (glitching, voltage manipulation) to test boot integrity and tamper resistance where feasible.
- **Power cycle / persistence testing.** Verifying that security-critical states (version counters, keys, configuration) persist correctly across power cycles.
- **Physical tamper detection.** Verification of physical tamper detection/evidence mechanisms on IoT devices and network equipment.
- **Pre-OS environment testing.** Specialised testing in the pre-operating-system environment, using JTAG debuggers, logic analysers and serial consoles.

5.4.7 Code and Binary Analysis

Static and dynamic analysis of source code and compiled binaries to identify security weaknesses, verify implementation correctness and confirm secure coding practices.

The draft vertical standards require source code access for several mitigations. MI-SSCA lists source code as both a required activity input and a required evidence item and is mandatory for 15 out of 17 security profiles in EN 304 626 (operating systems). MI-IMSL similarly requires source code as evidence. MI-FZ95 and MI-SCFS require build-system artefacts or instrumented builds that in practice presuppose source access. A CAB seeking notification for product categories where these mitigations apply must be competent to handle and assess source code.

- **Source code security review.** Static analysis for security vulnerabilities, insecure patterns, and memory errors (buffer overflow, out-of-bounds access, use-after-free, double-free, un-initialised variables, invalid pointer dereference). The assessor must review the source code, the analysis-tool output, and the documentation of warnings and suppressions, and verify that tool output is consistent with the source code.
- **Memory-safe language verification.** Where the manufacturer elects MI-IMSL (implemented in a memory-safe language) as an alternative to MI-FZ95 or MI-BTIN, a review of the source code to confirm the language used and to verify that all uses of unsafe memory features are documented and justified.
- **Binary analysis.** Analysis of production builds to verify security properties, absence of debug symbols and hardening flags (ASLR, stack overflow detection, heap protections, control flow integrity, write-or-execute enforcement, memory zeroing, reference-counter overflow mitigation, linked-list corruption prevention, separation of the kernel from user space memory).
- **Secure compilation flags verification.** Verification that security-relevant firmware and software is compiled with secure compilation flags appropriate to the platform and language, including review of build-system files and any documented exceptions.
- **Third-party security assessment.** Review of independent security assessments commissioned by the manufacturer, verifying scope adequacy and resolutions of findings.
- **Architecture review against threat model.** Verification that the implementation matches the documented security architecture and addresses identified threats.
- **Supply chain security review.** Analysis of third-party components, dependencies and build-pipeline integrity for supply chain risk.
- **Modification testing.** Testing manufacturer-specific modifications to upstream code, to ensure they do not introduce regressions or vulnerabilities.
- **Integration testing.** Validation that integrating upstream components with manufacturer additions maintains security and compliance.

NOTE: This competence category applies only to selected product categories within the scope of the CRA.

5.4.8 Process and Lifecycle Assessment

Review of development evidence supporting conformity of the product's technical design and development with Annex I, Part I, together with the manufacturer's vulnerability-handling processes under Annex I, Part II (Annex VIII, Part II, points 1 and 4.1). The activities below have been selected according to the product, risks and applicable requirements for assessment. The CRA does not require an SDLC, and the notified body does not assess whether the manufacturer operates one

- **Product development evidence review.** An examination of relevant development procedures, design rationale, security-testing records/results and other evidence supporting the adequacy of the product's technical design and development. Where the manufacturer uses an SDLC, its outputs may provide evidence; operating that framework is not a prerequisite for conformity assessment.

NOTE: Relevant draft vertical standards propose product-specific development and testing evidence, including the TR-SSDD requirement (evidence that static source code analysis (MI-SSCA), runtime coverage testing (MI-FZ95), boundary testing (MI-BTIN), or memory-safe language use (MI-IMSL) have been applied) and associated mitigations. Their applicability depends on the draft, product and security profile. They are referenced only to identify anticipated competence needs. They do not establish a general CRA requirement to operate an SDLC or an independent notified-body duty to assess whether one exists. Their treatment must remain consistent with the Commission guidance and the applicable legal requirements

- **Code review evidence verification**. The review of code-analysis findings and their resolution as evidence supporting product conformity; this is not a general audit of the manufacturer's code-review process
- **Security testing process review.** An assessment of whether the manufacturer's security tests and reviews are appropriate to the product and risks. Static analysis, dynamic analysis and penetration testing are possible methods, not the universal activities prescribed by the CRA (Annex I, Part II(3)).
- **Update testing process review.** A verification that updates are tested before distribution for compatibility and safety.
- **Risk assessment methodology.** A review of the manufacturer's methodology for assessing cybersecurity risk and its application to the product.
- **Conformity maintenance process.** An assessment of the processes to maintain conformity over time, including the monitoring for new vulnerabilities and regulatory changes.

5.4.9 Examination of Vulnerability Handling and Reporting

The manufacturer's vulnerability-handling processes are assessed against the CRA Annex I, Part II. prEN 40000-1-3 is the draft standard for horizontal vulnerability handling that will address these requirements. Relevant sectoral and product-specific standards may provide complementary methods or evidence. Their coverage must be assessed vis-a-vis the applicable provisions and any references to the horizontal standard, rather than presumed from their classification as horizontal or vertical.

- **SBOM verification.** A review of the Software Bill of Materials in a commonly used and machine-readable format for completeness, accuracy, the coverage of at least top-level dependencies and the identification of known vulnerable components.
- **Vulnerability disclosure process audit.** A review of the manufacturer's coordinated vulnerability disclosure (CVD) policy and process.
- **Patch/update delivery assessment.** Verification of the manufacturer's ability to deliver security updates promptly, including testing update distribution channels.
- **Support-period documentation review.** Verification that the manufacturer provides the required end-of-support information and, where technically feasible, an end-of-support notification mechanism (CRA Article 13(8) and (19), Annex II and Annex VII).
- **Vulnerability monitoring verification.** Confirmation that the manufacturer actively monitors for new vulnerabilities in their product and third-party components.

NOTE: Incident reporting (CRA Art. 14) is a separate operational obligation on a manufacturer and not an Annex I essential cybersecurity requirement that is assessed through Module B. Personnel may need to understand the reporting framework where related records inform evidence related to the handling of vulnerabilities. However, this does not constitute verification of Article 14 compliance.

5.4.10 Compliance Mapping and Evidence Aggregation

Cross-cutting activities that aggregate test results, map them to CRA requirements, and produce formal conformity documentation.

- **Mapping of controls with essential cybersecurity requirements.** Tracing each technical requirement to specific CRA Annex I essential requirements (Part I and Part II).

NOTE: The vertical standards include an informative Annex A mapping between standard requirements and CRA requirements.

- **Use case applicability mapping.** Determinations of which requirements apply based on product use cases, risk levels and deployment contexts.
  NOTE: Draft vertical standards define product-specific **Security Profiles** (SPs) that map product use cases and risk factors to the required sets of **Mitigations** (MIs). For example, draft ETSI EN 304 626 defines SP-IoT-2 for more complex or highly connected IoT operating systems, SP-RO-1 for lightweight, restricted or real-time operating systems, and SP-MOB-1 for consumer or enterprise mobile operating systems (such as smartphone and tablet platforms).
- **Evidence compilation.** Aggregation of all documentation, test, configuration, operational and process evidence into a conformity dossier.
- **Harmonised standard conformity verification.** Verifying, where the manufacturer claims harmonised standards have been applied, that the relevant standards have been correctly applied. Where standards have not been applied, or cover the requirements only partially, an assessment must be made as to whether the manufacturer's alternative solutions meet the corresponding essential requirements.
- **Non-conformity identification and corrective action.** Where the notified body finds that the product or the manufacturer's processes do not meet the essential requirements, it must formally document the non-conformity, communicate it to the manufacturer, and require corrective measures. The notified body must not issue a certificate until non-conformities are resolved.

Knowledge input. These testing activities should be read together with the emerging CRA framework for harmonised standards. The required technical competences can only be finalised once these standards are cited.

- **Horizontal standards (prEN 40000 series).** CRA standards under development, covering vocabulary (prEN 40000-1-1), cyber-resilience principles (prEN 40000-1-2) and vulnerability handling requirements in the CRA Annex I, Part II (prEN 40000-1-3).
- **prEN 40000-1-10.** Draft vertical standard for products with digital elements used in identity management systems and privileged access management software and hardware, including biometric readers.
- **prEN 40000-1-11.** Draft vertical standard for Hardware Devices with Security Boxes incorporating a physical envelope for hardware and designed to provide security functions such as secure storage and cryptographic operations in open environments.
- **Vertical (product-specific) standards (ETSI EN 304 6xx series).** Developed under standardisation request M/606, covering specific product categories in CRA Annexes III and IV (e.g. EN 304 626 for operating systems, EN 304 617 for browsers, EN 304 623 for boot managers, EN 304 636 for firewalls). These address CRA Annex I, Part I through product-specific Technical Requirements (TR-xxx) with associated Mitigations (MI-xxx), mapped to use cases and security profiles.

Source code access. A selection of draft vertical harmonised standards (e.g. EN 304 626) includes mitigations whose assessment criteria explicitly require the assessor to review the source code for the product. MI-SSCA (static source code analysis for memory errors) lists *the source code for the product* as both a required activity input and required item of evidence and is mandatory for 15 out of 17 security profiles in the OS standard. MI-IMSL (implement in a memory-safe language) similarly requires source code as evidence. A CAB seeking notification for product categories where these mitigations apply must be competent to handle and assess source code.

Applicability note. Not every activity applies to every product. The vertical standards use a risk-based structure, in which Technical Requirements map through Mitigations to Use Cases and Security Profiles. A CAB seeking notification must demonstrate competence across the testing categories relevant to the product families within the scope of its accreditation.

6 RED-Module B: CAB Technical Competences

6.1 Scope of Accreditation

According to EA-2/17 M: 2026, the main elements to be included in the scope of accreditation are the following.

a. The harmonised standard (HS) used as the accreditation reference and applied in full – here EN ISO/IEC 17065.
b. **The applicable legislation.** Directive 2014/53/EU (the RED Directive) and Commission Delegated Regulation (EU) 2022/30[15], concerning the application of the essential requirements in Article 3(3)(d), (e) and (f).
c. **The conformity assessment procedure used.** RED Annex III, Module B: EU-type examination.
d. **The radio-equipment categories or families covered**, identified together with the applicable RED essential requirement under Article 3(3)(d), (e) or (f), as specified by Article 1 of Commission Delegated Regulation (EU) 2022/30:
   - **Article 3(3)(d)** concerns radio equipment capable of communicating over the internet, directly or through other equipment;
   - **Article 3(3)(e)** applies where the equipment processes personal, traffic or location data:
     - internet-connected radio equipment other than the categories listed below;
     - radio equipment designed or intended exclusively for childcare;
     - radio equipment covered by Directive 2009/48/EC (Toy Safety Directive);
     - radio equipment designed or intended, whether exclusively or not, to be worn on, strapped to, or hung from the human body or clothing;
   - **Article 3(3)(f)** refers to internet-connected radio equipment enabling the holder or user to transfer money, monetary value or virtual currency.

   The scope of the accreditation should identify both the relevant product family and the applicable RED 3(3) directive, or requirements due to overlapping categories and where differing requirements for competence and different technical standards may apply. The exclusions in Article 2 of Delegated Regulation (EU) 2022/30 must also be considered.
e. **The applicable product characteristics or specifications.** These are the relevant RED essential requirements and, where applicable, the corresponding harmonised standards, including the relevant parts of the EN 18031 series and any limitations or restrictions attached to their citation in the Official Journal.

A CAB notified for RED Module B must demonstrate the capability to undertake each of the following:

1. **assess the adequacy of the technical design of radio equipment**, including the relevant technical documentation and supporting evidence;
2. **assess conformity of the technical design with the applicable essential requirements of Article 3 of Directive 2014/53/EU**;
3. **perform these conformity assessment activities with the required independence, impartiality, competence and consistency**.

[15] European Commission. Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. *Official Journal of the European Union*, 12 January 2022, L 7, pp. 6–13.

6.2 Standards for Accreditation for Notification

According to the EA Accreditation for Notification (AfN) Project Report (May 2026, Annex C), accreditation for RED Annex III, EU-type examination (Module B) is based on **EN ISO/IEC 17065**. EA identifies EN ISO/IEC 17065 as the preferred standard because it covers all aspects of the EU-type examination and links to other relevant conformity-assessment standards through Clause 6.2. The corresponding 2026 obligatory-standard approach is set out in EA-2/17 M:2026, Annex A, with *cd+pk+t* requirements and the transition described in Section 1.2.

6.3 Competence Requirements for RED-Module B Notified Bodies

The tables below list the competence requirements for RED-Module B Notified Bodies, related to the scope of accreditation, organised by the three requirement categories introduced in Section 3. Section 6.4 (Competence Requirements by Conformity Assessment Activity) details the competence requirements related to the type of conformity assessment activity.

Table 9. RED-Module B: Specific requirements related to the scope of accreditation

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCE
Product-specific conformity assessment capability	Capability to assess the adequacy of the technical design and development of internet-connected radio equipment	EN 18031-1:2024, clause 1

Table 10. RED-Module B: Specific requirements related to the type of conformity assessment activity

AREA OF COMPETENCE	REQUIREMENTS	STANDARD REFERENCES
Competence to perform IT security testing	Documentation and Conceptual Review; Functional Security Testing; Configuration & Settings Inspection; Vulnerability Analysis *(limited)*; Cryptographic Validation; Physical and Hardware Security Testing; Compliance Mapping & Evidence Aggregation	EN 18031:2024, clause 6
Competence to execute testing activities in a competent, independent, and reproducible manner	**Applicable where testing is required.** The body must demonstrate the relevant ISO/IEC 17025 competence for the tests it performs or commissions within its conformity assessment procedure.	EA-2/17 S1 M:2026, Table 1 and Key ‘t’ (CRA Annex VIII, Part II); applicable clauses 6 and 7 of ISO/IEC 17025:2017, excluding 7.9
Capability to examine the manufacturer’s vulnerability-handling processes, to attest fulfilment of the essential cybersecurity requirements of CRA Annex I, Part II	Not applicable to RED Notified Bodies	EA-2/17 S1 M:2026, Table 1 and Key ‘pk’, referencing EN ISO/IEC 17020:2012, clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; ISO/IEC 30111:2019; ISO/IEC 29147:2018
Outsourced capabilities	Subcontracting requirements as per the standard	ISO/IEC 17065:2012, clause 6.2.2

6.4 Competence Requirements by Conformity Assessment Activity

This section sets out the testing and evaluation activities that define the technical competence required of a RED notified body (NB) performing Module B (EU-type examination). The activities derive from the essential requirements in Article 3(3)(d), (e) and (f) as specified in Delegated Regulation (EU) 2022/30, the harmonised standard EN 18031 series (EN 18031-1 to -3) and the Module B examination procedure in Annex III.

Determination methods. A RED notified body determines conformity through the following actions.

1. **Examining the manufacturer's documentation** and **decision-tree paths** for each applicable EN 18031 mechanism, to assess the adequacy of the technical design against the essential requirements in Art. 3(3)(d), (e), and (f). This activity does not require the equipment to be operational (***conceptual*** assessment).
2. **Verifying**, by means such as scanners and analysers, that the **manufacturer's documentation** of the technical design is **complete** and that **no undocumented items have been omitted**. The reference standard does not prescribe specific techniques for this activity (***completeness*** assessment).
3. **Carrying out** – or arranging for – **active**, often adversarial, **testing** (attack simulation, fuzzing, exploitation) to check that the manufacturer's implementation is adequate to meet the corresponding essential requirement. Techniques are left to the notified body to define (***sufficiency*** assessment).
4. **Determining**, for each specimen, **which EN 18031 part(s) apply**, based on the asset types present (network, privacy or financial), the equipment category (internet-connected, childcare, toy, wearable, financial-processing) and the decision-tree outcome for each mechanism.

NOTE: Not every activity in points 1–3 applies to every product; applicability is established through the determination in point 4. A CAB seeking notification must demonstrate competence across the testing categories relevant to the product families within its accreditation scope.

6.4.1 Documentation and Conceptual Review

Review of manufacturer-provided technical documentation to verify that security mechanisms are properly designed, justified and traceable without requiring the equipment to be operational.

- **Security and functional asset identification review** (Conceptual; ACM-1, SSM-1, SCM-1). An examination of the manufacturer’s identification of all security-relevant assets (security, network and where applicable privacy or financial assets) for completeness and cross-mechanism consistency.
- **Security mechanism applicability review** (Conceptual; ACM-1, AUM-1, SUM-1, SSM-1, SCM-1). Reviews of the manufacturer’s determination of applicability for each family of mechanisms (access control, authentication, secure update, secure storage and secure communication).
- **Security mechanism design review** (Conceptual; ACM-2, AUM-2–6, SUM-2/3, SSM-2/3, NMM-1, RLM-1, TCM-1, GEC-2/4/8). An examination of the documented design and rationale across access control, authentication, brute-force protection, secure update, secure storage, secure communication, network monitoring, resilience, traffic control, interface exposure reduction and boot integrity.
- **Privacy-specific access review** (Conceptual; ACM-3–6). Reviews of the documented default access setup for child and parental controls, for products within the scope of EN 18031-2.
- **Logging mechanism design review** (Conceptual; LGM-1–4). Reviews the documented logging mechanisms for privacy-relevant (Part 2) or financial-relevant (Part 3) activities, including event types, exclusions and data minimisation in logs.

- **Privacy-specific design review** (Conceptual; DLM-1, UNM-1, GEC-7). Reviews documented data deletion and user-notification mechanisms, and documentation of external sensing capabilities.
- **Known vulnerability documentation review** (Conceptual; GEC-1). Reviews the manufacturer's list of known publicly-exploitable vulnerabilities, remediations, mitigations and risk acceptances.
- **Cryptographic key design review** (Conceptual; CCK-1–3). Reviews documented confidential cryptographic keys, their security strength, generation mechanisms and prevention of static default values.
- **Cryptography best-practice review** (Conceptual; CRY-1). An examination of documented cryptographic schemes and algorithms against applicable EUCC/ENISA state-of-the-art documents and recognised European, national or international cryptographic catalogues, including BSI, NIST and ETSI references where relevant.
- **Decision-tree path verification** (Conceptual; all mechanisms). A systematic verification of all documented decision-tree paths and the justifications for consistency and completeness.
- **Threat and risk assessment review** (Conceptual; all mechanisms). Reviews the manufacturer's threat modelling, risk assessment and risk treatment decisions.

6.4.2 Functional Security Testing

Active testing of security mechanisms to verify documentation completeness (Completeness tier) and implementation adequacy (Sufficiency tier).

- **Access control mechanism discovery and testing** (Completeness/Sufficiency; ACM-1/2). An active identification of all assets accessible by entities, verified against documentation, followed by a confirmation that the mechanisms are functional and effective.
- **Privacy-specific access control testing** (Sufficiency; ACM-3, Part 2 only). Testing that default restrictions on children's access and parental controls are effective and conform to design.
- **Authentication interface discovery and testing** (Completeness/Sufficiency; AUM-1–6). Identification of all interfaces providing access to protected assets, followed by verification of authentication enforcement, password validation and strength, certificate validation, brute-force protection and authenticator change protection.
- **Update mechanism discovery and verification testing** (Completeness/Sufficiency; SUM-1/2). Identification of all update mechanisms and delivery channels, followed by verification of update signatures, secure channel delivery, access control and automated mechanisms.
- **Secure storage mechanism discovery and testing** (Completeness/Sufficiency; SSM-1/2/3). Identification of all stored assets requiring protection, followed by confirmation of integrity (digital signatures, tamper detection) and of protection confidentiality, including hardware-protected storage.
- **Secure communication mechanism discovery and testing** (Completeness/Sufficiency; SCM-1–4). The identification of all communicated assets and channels, followed by confirmation of the protection of confidentiality, integrity and authenticity, including resistance to man-in-the-middle, eavesdropping and replay tactics.
- **Privacy/financial event logging testing** (Completeness/Sufficiency; LGM-1–4, Parts 2/3 only). Verification that logged event types are complete and that logging mechanisms correctly record relevant activities, including log persistence, storage and time-stamping.
- **Personal data storage discovery and deletion testing** (Completeness/Sufficiency; DLM-1, Part 2 only). The identification of all locations where personal data is stored, followed by verification that deletion is complete, resilient, tamper-resistant and simple to activate.
- **User notification mechanism testing** (Sufficiency; UNM-1, Part 2 only). Verification that notifications for privacy-relevant events are operational, appropriate, timely and contain the relevant content.

- **Resilience mechanism discovery and DoS testing** (Completeness/Sufficiency; RLM-1). The identification of all network interfaces and resilience mechanisms, followed by simulated denial-of-service attacks (flooding, protocol fuzzing, application scanning) and verification of recovery.
- **Boot process completeness verification** (Completeness; GEC-8, Part 3 only). The verification that all boot integrity processes are documented, with no undocumented boot stages.

6.4.3 Configuration and Default-State Inspection

Examination of the equipment's configuration in factory-default and operational states.

- **Factory default interface exposure audit** (Completeness; GEC-2). The verification that only interfaces and services necessary for setup or basic operation are exposed by default, using scanning tools.
- **Optional service configuration audit** (Sufficiency; GEC-3). The verification that optional services can be enabled or disabled and that disabled services are inaccessible.
- **Exposed interface documentation completeness** (Completeness; GEC-4). The comparison of documented interfaces against those found through active scanning.
- **Unnecessary external interface assessment** (Completeness; GEC-5). An assessment to ensure that every physical and logical interface serves an operational purpose.
- **External sensing capability verification** (Completeness; GEC-7, Part 2 only). A verification that all privacy-affecting sensing interfaces (microphone, camera etc) are documented in user documentation.

6.4.4 Vulnerability Analysis

Assessment of the equipment's vulnerability status and input-validation resilience.

- **Known-vulnerability scanning** (Completeness; GEC-1). A search using up-to-date tools for known vulnerabilities, cross-referenced against the manufacturer's documented list.
- **Vulnerability remediation/mitigation verification** (Sufficiency; GEC-1). The verification that documented remediation or mitigation measures are correctly implemented, or that non-exploitability conditions are effective.
- **Risk acceptance justification review** (Conceptual; GEC-1). Review of risk-based justifications for the acceptance of unremediated vulnerabilities.
- **Input method discovery and injection/fuzzing testing** (Completeness/Sufficiency; GEC-6). Enumeration of all input methods on external interfaces, followed by SQL/Ajax/OS command injection, path traversal and fuzzing testing (mandated explicitly by GEC-6 sufficiency assessment).
- **Man-in-the-middle and replay-attack simulation** (Sufficiency; SCM-2/4). Simulated interception, tampering and replay of communications to verify integrity, authenticity and replay-rejection.
- **DoS and brute-force attack simulation** (Sufficiency; RLM-1, NMM-1, AUM-6, Part 1 only for network DoS). Simulated flooding/fuzzing attacks and brute-force authentication attacks to verify resilience and protection at scale.

6.4.5 Cryptographic Validation

- **Best-practice cryptography assessment** (Conceptual; CRY-1). Verification of cryptographic schemes and algorithms against recognised reference catalogues.
- **Cryptographic-implementation and key discovery** (Completeness; CRY-1, CCK-1). Identification of any undocumented cryptography or confidential keys.

- **Cryptographic-implementation conformance testing** (Sufficiency; CRY-1). Verification that actual implementation matches documentation (algorithms, key sizes, protocol modes) and that key length and strength conforms to requirements.
- **Key-generation mechanism assessment** (Sufficiency; CCK-2). An assessment against best practices in the generation of random numbers; verification that pre-installed keys are unique, not static defaults.
- **Cryptographic-communication and storage testing** (Sufficiency; SCM-2/3, SSM-3). Verification of cryptographic protections within communication mechanisms and of stored-data encryption.
- **Boot integrity and chain-of-trust verification** (Sufficiency; GEC-8, Part 3 only). The verification of cryptographic boot integrity via an immutable or protected root of trust to validate the full chain of trust.

6.4.6 Physical and Hardware Security Testing

Testing activities involving hardware security features. GEC-8 applies only to Part 3 (financial asset protection).

- **Hardware-backed storage integrity testing** (Sufficiency; SSM-2). Confirmation that hardware-based integrity mechanisms prevent unauthorised modification of stored assets.
- **Hardware-backed storage confidentiality testing** (Sufficiency; SSM-3). Confirmation that hardware-protected storage prevents extraction of confidential data.

6.4.7 Code and Binary Analysis

NOTE: EN 18031 does not impose source-code review or binary analysis as standalone assessment activities. Its methodology is based principally on conceptual assessment, documentation review, and functional completeness and sufficiency testing. A CAB may nevertheless use binary inspection, protocol-analysis or similar tools where they support an applicable assessment – for example, input-validation testing under GEC-6 or cryptographic assessment under CRY-1. In such cases, these tools support the EN 18031 assessment rather than constituting independently mandated activities.

While the CRA does not name source-code review or binary analysis either, its open-ended, risk-based requirements (no known exploitable vulnerabilities; effective and regular tests and reviews) make these techniques a realistic necessity for many products, in a way that EN 18031's closed mechanism catalogue does not require.

6.4.8 Process and Lifecycle Assessment

NOTE: RED Module B and EN 18031 are predominantly product focused. Systematic assessment or periodic auditing of the manufacturer’s vulnerability-handling and lifecycle processes are not required. This is a material structural difference from CRA Module B, which covers both the product’s cybersecurity characteristics under Annex I, Part I and the manufacturer’s vulnerability-handling processes under Annex I, Part II, including periodic auditing under Annex VIII, Part II, point 8.

6.4.9 Examination of Vulnerability Handling and Reporting

NOTE: RED and EN 18031 do not provide an equivalent to the CRA’s comprehensive vulnerability-handling framework. EN 18031 GEC-1 assesses the product’s vulnerability status only at the time of assessment by assessing documented product components, publicly-known exploitable vulnerabilities and relevant mitigations. However, it does not require systematic assessment and periodic auditing of the manufacturer’s ongoing vulnerability-management capability, including SBOM maintenance, coordinated vulnerability disclosure and continuous vulnerability monitoring throughout the support period.

This is one of the most significant scopes of differences between the RED and CRA. The CRA Annex I, Part II establishes eight lifecycle requirements for handling vulnerabilities. A CAB qualified only for EN 18031 would therefore need additional competence to assess these processes.

6.4.10 Compliance Mapping and Evidence Aggregation

Cross-cutting activities that aggregate assessment results and produce formal conformity documentation.

- **Essential-requirements mapping.** Tracing each verdict on an assessment to the applicable RED essential requirements.
- **Mechanism-applicability determination.** Formal determination of the mechanisms and requirements that apply, based on equipment functionality and operational environment.
- **Asset-scope determination.** A determination of the asset types that define the assessment boundary for the specific equipment.
- **Assessment-verdicts aggregation.** A compilation of all individual verdicts across assessment tiers into a consolidated conformity result.
- **Evidence-dossier compilation.** An aggregation of evidence, assessment records, test results and justifications into a structured conformity dossier.
- **Cross-standard mapping.** Where applicable, a mapping of the results to related standards for a potential reuse of evidence.

6.5 RED – CRA Module B Gap Analysis and Competence Comparison

CRA and RED Module B are both **based on the EN ISO/IEC 17065** certification framework, **supplemented** by the applicable legislative and activity-specific requirements. The analysis focuses on the following **areas of competence.**

- **Product-category/family competence** (partial alignment). The RED cybersecurity scope is limited to the categories in Delegated Regulation (EU) 2022/30. These include internet-connected radio equipment under Article 3(3)(d); internet-connected radio childcare equipment, toys and wearables that are capable of processing personal, traffic or location data, under Article 3(3)(e); and internet-connected radio equipment enabling transfers of money, monetary value or virtual currency under Article 3(3)(f).
- **Competence to perform IT security testing** (partial alignment). Detailed competence gaps analysed in Section 6.6.
- Competence to examine vulnerability-handling processes. Not applicable to RED Notified Bodies.
- **General testing competence under ISO/IEC 17025.** Applicable where testing is required under either framework. The CRA extension concerns the scope of the product, methods and personnel competence needed for the requested assessment activities.

The table below provides a comparative mapping of the competence, accreditation, structural and process requirements applicable to CABs performing CRA and RED conformity assessment activities, against the corresponding requirements applicable to RED Notified Bodies.

Table 11. CRA and RED-Module B CAB Competence and Accreditation Requirements

AREA OF COMPETENCE	CRA REFERENCE REQUIREMENTS	RED REFERENCE REQUIREMENTS
Scope-specific competence		

AREA OF COMPETENCE	CRA REFERENCE REQUIREMENTS	RED REFERENCE REQUIREMENTS
Assessment of technical design and development within the product category/family in scope	CRA Article 32(1) – (3); Annex VIII, Part II; Annexes III and IV where relevant to the product category	EN 18031-1:2024, clause 1
Conformity-assessment activity competence		
IT security testing	CRA Annex I, Part I	EN 18031:2024, clause 6
Competent, independent and reproducible execution of testing activities	ISO/IEC 17025:2017, clauses 6.1–6.5, 7.1–7.8, 7.10–7.11	Applicable ISO/IEC 17025:2017 clauses 6 and 7, excluding 7.9, where testing is required (EA-2/17 M:2026, Annex A, t)
Examination of manufacturer vulnerability-handling processes	EA-2/17 S1 M:2026, Table 1 and Key ‘pk’, referencing EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; ISO/IEC 30111:2019; ISO/IEC 29147:2018	**Not applicable to RED Notified Bodies**
Outsourced conformity-assessment activities	ISO/IEC 17065:2012, clause 6.2.2	ISO/IEC 17065:2012, clause 6.2.2
Structural and process requirements		
General requirements	ISO/IEC 17065:2012, clause 4	ISO/IEC 17065:2012, clause 4
Structural requirements	ISO/IEC 17065:2012, clause 5	ISO/IEC 17065:2012, clause 5
Process requirements	ISO/IEC 17065:2012, clause 7	ISO/IEC 17065:2012, clause 7
Management system requirements	ISO/IEC 17065:2012, clauses 8.2–8.8; ISO 9001:2015	ISO/IEC 17065:2012, clauses 8.2–8.8; ISO 9001:2015

6.6 IT Security Assessment Capability Gap Analysis: CRA and RED

This section lists, item by item and with regulatory citations, the IT-security testing capabilities CRA requires that EN 18031 (RED) does not and vice versa, then summarises the resulting qualification gap a CAB would need to close when moving in either direction.

6.6.1 Capabilities Required by CRA But Absent from RED

A CAB qualified only for an EN 18031 assessment would need to develop or demonstrate the following additional capabilities to perform CRA conformity assessments.

- **Source code security review** (CRA Annex I, Part I(2)(k)). EN 18031 focuses on product behaviour and documentation and has no equivalent requirement.
- **Binary hardening analysis** (CRA Annex I, Part I(2)(k), Part I(1)). Verification of exploitation mitigations, such as ASLR, stack canaries, DEP and CFI, require binary-level analysis and

specialised tooling. EN 18031 does not provide equivalent coverage, as it assesses only at the functional interface level.

- **Supply-chain security review** (CRA Annex I, Part II (1); Art. 13(5)). The CRA requires the generation and maintenance of SBOM and third-party component analysis. EN 18031 addresses known vulnerabilities (GEC-1) but not supply-chain provenance.
- **Development-evidence assessment** (CRA Annex I, Part I (1); Annex VII; Annex VIII, Part II, points 1, 3.4 and 4.1). Assessment of evidence demonstrating how identified cybersecurity risks have been addressed in the product's technical design and development. This may include relevant SDLC procedures and records, but the CRA does not require an SDLC, and the notified body does not assess whether the manufacturer operates one.
- **Coordinated-vulnerability-disclosure audit** (CRA Annex I, Part II(5)/(6)). The CRA requires auditable processes for coordinated vulnerability disclosure (CVD) and vulnerability handling. EN 18031 has no equivalent process-level requirement.
- **Vulnerability-monitoring verification** (CRA Annex I, Part II(2)/(7)). The CRA requires ongoing monitoring and timely remediation processes. EN 18031 (GEC-1) provides point-in-time vulnerability assessment.
- **Support-period documentation review** (CRA Art. 13(8)/(19)). The CRA requires manufacturers to determine and communicate the product's support period and make security updates available throughout that period. The notified body does not certify the manufacturer's determination of the support period as a separate essential requirement. Relevant competence concerns reviewing the information on the support period contained in the technical documentation and user information and its consistency with the evidence of actual conformity in practice. RED Module B has no comparable support-period regime; its continuing obligations concern modifications to the approved type and developments in the state-of-the-art.
- **Debug-interface testing** (CRA Annex I, Part I(2)(j)). The CRA requires security assessment of the JTAG/serial-console interfaces. EN 18031 (GEC-5) operates at the functional-interface level.
- **Fault-injection testing** (CRA Annex I, Part I(1), and (2)(d)/(f)/(j)/(k) as relevant to the threat scenario). Such testing may be necessary where the assessment of product risk identifies credible physical attack paths, for example through accessible JTAG, serial-console or other debug interfaces. EN 18031 does not address resistance to physical attacks.
- **Physical and hardware-security testing** (CRA Annex I, Part I(2)(d), (j) and (k) where applicable). The CRA does not require physical testing for every product. Depending on the product category, identified risks and applicable technical specifications, assessment may include specific assessment activities for debug-interface protection (MI-PDDI-1 to -4) and physical tampering or resistance to hardware attacks. EN 18031 provides a limited related foundation through secure-updates, boot-integrity (Part 3) and storage protection (SSM-2/3) but does not establish a comprehensive methodology for testing physical security.
- **Isolation-mechanism testing** (CRA Annex I, Part I(2)(k)). The CRA may require assessment of process, container or virtual machine (VM) isolation mechanisms. EN 18031 does not assess isolation boundaries.
- **Data-minimisation assessment** (CRA Annex I, Part I(2)(g)). The CRA extends existing EN 18031-2 competence in personal-data handling and minimisation of logged information to assess whether all data processed by the product are adequate, relevant and limited to what is necessary for its intended purpose.

6.6.2 Capabilities Required by RED but Absent from CRA Vertical Standards

A CAB qualified only for CRA assessment would need the following additional capabilities for EN 18031 conformity assessment.

- **Network-monitoring mechanism testing** (required by RED Art. 3.3(d)). EN 18031-1 requires testing traffic-monitoring mechanisms (GTP filtering, IP packet filtering, anomaly detection).

CRA addresses DoS resilience (Annex I, Part I(2)(h)) but does not require network monitoring capabilities in the equipment itself.

- **Traffic-control mechanism testing** (required by RED Art. 3.3(d)). EN 18031-1 requires testing of datagram filtering rules and traffic separation mechanisms. CRA's related provision (Part I(2)(i)) does not require active traffic-control testing.
- **External-sensing capability-documentation verification** (required by RED Art. 3.3(e)). EN 18031-2 requires verifying all sensing capabilities (cameras, microphones) are documented. There is no CRA equivalent (CRA's data-minimisation requirement in Annex I, Part I (2)(g) is related but does not require disclosure of sensing hardware).
- **User-notification mechanism testing** (required by RED Art. 3.3(e)). EN 18031-2 requires testing that users are notified of privacy-relevant events with appropriate content. CRA's closest equivalent is the requirement for recording general security information (Part I(2)(l)).
- **Boot integrity and chain-of-trust verification, financial-asset framing** (required by RED Art. 3.3(f)). EN 18031-3 GEC-8 (Part 3 only) requires verification that equipment cryptographically verifies software integrity during boot using an immutable or protected root of trust, and that the chain of trust validates each component. EN 18031-3 defines boot integrity as a specific requirement for the protection of financial assets with completeness and sufficiency tiers. While CRA also covers boot integrity, the RED Part 3 framing ties it specifically to the security of financial transactions, requiring the CAB to assess it in that context.
- **Privacy and financial event logging testing** (required by RED Art. 3.3(e)/(f)). EN 18031-2 (LGM-1–4) requires testing the logging of specific asset types (privacy, financial) with defined completeness/sufficiency tiers. CRA's logging requirement is general and does not mandate the verification of the logging of specific asset types.
- **Structured decision-tree assessment** (required by RED Art. 3.3(d)/(e)/(f)). EN 18031's prescriptive decision-tree and evidence-element methodology is a structural feature that demands a specific type of competence in systematic assessment. CRA vertical standards use a category-based approach without this prescriptive logic.

6.6.3 Capabilities Required by both Frameworks with Material Scope Differences

- **Penetration testing.** The CRA product assessment addresses Annex I, Part I(2)(a) and, where relevant to the product and risks, points (j) and (k). The required methods and depth depend on the product, the identified risks and applicable technical specifications; penetration testing is not a uniform activity prescribed for every product. EN 18031 uses adversarial testing, within the assessment of mechanism-specific sufficiency, providing a relevant foundation. A CAB transitioning from EN 18031 to the CRA may need to extend this to broader product-level vulnerability analysis and penetration testing. Additionally, Annex I, Part II(3) requires the manufacturer to undertake regular security tests and reviews; the notification body assesses that process rather than assuming a general obligation to perform continuous lifecycle penetration testing.
- **Vulnerability scanning.** Both require CVE-level scanning against public databases. The CRA (Annex I, Part I (2)(a) and Part II (1)) additionally mandates SBOM-based dependency scanning, ongoing monitoring and third-party component analysis, whereas EN 18031 (GEC-1) scans are point-in-time only.
- **Cryptographic assessment.** EN 18031 (CRY-1) is more prescriptive, referencing recognised cryptographic catalogues and technical guidance. The CRA Annex I, Part I (2)(e) uses broader state-of-the-art language. The CRA draft vertical standards additionally identify protocol-level activities such as TLS-compliance, random-number-generation and VPN-tunnel testing, whereas EN 18031 treats these within the assessment of mechanism-specific sufficiency.
- **Secure-update testing.** Closely aligned at the product level, CRA (Annex I, Part I (2)(c) and Part II (7)) additionally requires the testing of protections for rollbacks and assessments of the manufacturer's infrastructure for distributing updates, whereas EN 18031 (SUM-1/2/3) tests only the equipment's update mechanism.

- **Logging and audit testing.** EN 18031 is more detailed on logging requirements (retention minimums, persistence, timestamping) and limits scope to privacy and financial events. The CRA (Annex I, Part I (2)(l)) additionally requires a user opt-out mechanism and covers logging of access to or modification of data, services or functions more broadly.
- **Data-deletion testing.** Both require the testing of deletion mechanisms. EN 18031 is more prescriptive on robustness (resilience against interruption, tamper resistance). The CRA (Annex I, Part I (2)(m)) additionally requires secure transfer of data to other products.
- **Default-configuration testing.** Both require the verification of factory-default states; The CRA (Annex I, Part I (2)(b)) additionally requires the ability to reset to original state (factory reset) as a distinct test. EN 18031 (GEC-2/3/5) does not explicitly test this as a distinct activity and is more prescriptive about what constitutes acceptable exposure to default states.
- **Resilience/DoS-protection testing.** EN 18031 (RLM-1) is more prescriptive on tools and methodology for network equipment. The CRA (Annex I, Part I (2)(h)) applies DoS resilience to all products with digital elements, not just network equipment, so a CRA CAB may need to test DoS resilience on software products without network interfaces.
- **Attack-surface minimisation verification.** The scope of the CRA (Annex I, Part I (2)(j)) is broader, extending to code-level attack surfaces (debug symbols, unused code paths) and hardware (debug ports). EN 18031 (GEC-2/4/5) limits this to network-accessible interfaces and services.
- **Boot-integrity testing.** EN 18031 (GEC-8) is more prescriptive (requires immutable or crypto-authorised root of trust) but limited to financial-data equipment (Part 3). The CRA (Annex I, Part I (2)(f)) does not mandate boot integrity for all products, but its requirements for integrity protection and the mitigation of exploitations can imply it for high-risk products more broadly.

6.6.4 Qualification Gap Synthesis

The capability gaps identified above translate into the following additional qualification requirements for CABs transitioning between the two frameworks.

For a RED CAB seeking CRA qualification additional qualification is required in areas including the following.

- **Code and binary analysis.** Source code review, binary hardening verification (CRA Annex I, Part I(1), (2)(a), (k), Part II (3)).
- **Product development evidence and vulnerability handling process assessment**. Review of evidence supporting the product's conformity with Annex I, Part I, and assessment of the manufacturer's processes for handling vulnerabilities under Annex I, Part II, including vulnerability monitoring, remediation and SBOM-related evidence. The existence of an SDLC is not an assessment criterion. Periodic audits cover the implementation of vulnerability-handling processes only (CRA Annex VII; Annex VIII, Part II, points 1, 4.1 and 8).
- **Physical and hardware-security testing**. Where justified by the product category, intended purpose and use environment, the manufacturer's cybersecurity risk assessment, the product's attack surface and the applicable technical specifications including, where relevant, physical attack vectors are identified, competence in debug-interface security, physical tampering and specialist hardware-attack techniques are required (CRA Annex I, Part I(2)(d), (j) and (k)).
- **Isolation and containment testing.** Process isolation, sandboxing and container/VM separation (CRA Annex I, Part I(2)(k)).
- **Data-minimisation assessment**. An assessment of whether the personal and other data processed by the product are adequate, relevant and limited to what is necessary for its intended purpose (CRA Annex I, Part I(2)(g)). EN 18031-2 provides a related competence base through personal-data protection and minimisation of logged information. The extension needed depends on the CAB's existing scope and demonstrated competence.
- **Vulnerability-analysis methodology**. The selection and application of appropriate product-level vulnerability-analysis methods, building on EN 18031 GEC-1 checks for publicly-known

exploitable vulnerabilities. The methods and depth, including penetration testing where justified, depend on product risks, applicable standards or specifications and the notified body's assessment procedures. The CRA prescribes no single method (Annex I, Part I(2)(a) and, where relevant, (j) and (k)).

- **Support-period documentation review.** Verification that the manufacturer has documented the information used to determine the support period in the technical documentation and has clearly communicated the end date of that period to users and, where technically feasible, notifies users when the product reaches the end of its support period (CRA Article 13(8), Annex VII and Annex II (CRA Art. 13(8) and (19)).

For a CRA CAB seeking RED qualification additional competence is required in areas that include the following.

- **Children's safety and privacy testing for toys and childcare equipment** – driven by RED Art. 3.3(e).
- **Testing for privacy-relevant or financial-data-processing equipment** – driven by RED Art. 3.3(e) and 3.3(f).
- **Network monitoring and traffic-control testing** – driven by RED Art. 3.3(d)
- **External sensing capability documentation** – driven by RED Art. 3.3(e).
- **User notification mechanism testing for privacy events** – driven by RED Art. 3.3(e).
- **Structured decision-tree and evidence-element assessment methodology**.

Structural differences requiring adaption of the scope or methodology are as follows.

The RED requires mechanism-by-mechanism assessment with three formal tiers (conceptual, completeness, sufficiency) and pass/fail verdicts, demanding structured workflows with formal evidence handling.

The CRA requires assessment organised by testing-capability category, relying on broader professional judgement, demanding holistic security assessment expertise.

The RED is purely product-focused. The CRA extends assessment to manufacturer processes, ongoing operations and lifecycle management.

7 EUCC: CAB Technical Competences

7.1 Scope of Accreditation

The EUCC splits the CAB functions between the **IT Security Evaluation Facility** (**ITSEF)**, which performs the technical evaluation, and the **certification body** (CB), which reviews the evaluation results and makes the certification decision. Their accreditation scopes are therefore defined separately.

For the ITSEF – under the ENISA EUCC State-of-the-Art document (SotA) *Accreditation of ITSEFs for the EUCC Scheme*[16], Sections 4, 5 and 6, the accreditation scope must at least specify the following.

a. **The testing field.** ICT cybersecurity evaluation.
b. **The test object, product or process.** ICT products within the following categories:
   - smartcards and similar devices;
   - hardware devices with security boxes;
   - generic software and network products.
c. **The assurance components.** the ISO/IEC 15408-3 in which the ITSEF has proven technical competence to evaluate in line with ISO/IEC 18045:2022, for example, evaluation up to EAL3 augmented with ALC_FLR.2.
d. **The certification scheme**. EUCC.

The types of technology and evaluation techniques from Annex A for which the ITSEF has demonstrated competence must be detailed in the accreditation assessment report. These include technology domains such as operating systems, application security, network and wireless technologies, secure microcontrollers and smartcards, and evaluation techniques such as source-code review, cryptographic analysis, vulnerability analysis and penetration testing.

The SotA of the ITSEF must expressly identify these minimal elements in its scope and distinguish them from the additional details on competence recorded in the assessment report.

For the CBs, under the ENISA EUCC SotA *Accreditation of CBs for the EUCC Scheme*[17]*,* Sections 5 and 6, the scope shall at least specify the following.

a. **The certification field.** ICT cybersecurity evaluation.
b. **The certification object, product or process.** ICT products within the following categories:
   - smartcards and similar devices;
   - hardware devices with security boxes;
   - generic software and network products.
c. **The assurance components.** ISO/IEC 15408-3 in which the CB has proven technical competence to review the assessments and reports established by the ITSEFs in line with ISO/IEC 18045:2022, for example, certification up to EAL3 augmented with ALC_FLR.2.
d. **The certification scheme**. EUCC.
e. **The technology and evaluation technique types**, per Annex A of the SotA, detailed in the accreditation assessment report rather than in the statement of scope itself.

The types of technology and evaluation techniques for which the CB has demonstrated competence must be identified in the accreditation assessment report. Unlike an ITSEF, a CB does not necessarily need the capability or equipment to conduct specialised attacks, but it must understand the relevant methods sufficiently to review the work of the ITSEF and make a competent decision on certification.

[16] EUCC Scheme, State-of-the-Art Document, Accreditation of ITSEFs for the EUCC scheme, Version 1.6c, November 2024, available from https://certification.enisa.europa.eu/publications/.
[17] EUCC Scheme, State-of-the-Art Document, Accreditation of CBs for the EUCC scheme, Version 1.6b, November 2024, available from https://certification.enisa.europa.eu/publications/.

The scope of accreditation should identify the **ISO/IEC 15408-3 assurance components for which competence has been demonstrated**, expressed through the applicable Evaluation Assurance Level and any augmentations, for example, **EAL3 augmented with ALC_FLR.2**.

This scope determines the evaluations an ITSEF may perform and the evaluation results a CB may review and certify under the EUCC. EUCC certificates may be issued at:

- **Assurance level 'substantial'**, i.e. generally associated with EAL1–EAL3 and AVA_VAN.1–AVA_VAN.2;
- **Assurance level 'high'**, i.e. generally associated with EAL4–EAL7 and AVA_VAN.3–AVA_VAN.5.

A CAB notified for the EUCC must demonstrate the capability to:

1. **evaluate the target of evaluation** (ICT product or protection profile) **against its Security Target**, specific to the technical domain and assurance components in the scope as held by the **ITSEF**, not by 'the CAB' generically;
2. **assess fulfilment of the applicable Common Criteria assurance requirements** (not the 'essential requirements' in the CRA/RED product-legislation sense) and to issue the certification decision held by the **certification body** reviewing the ITSEF's technical evaluation report;
3. **sustain impartiality, independence and consistent operation** which applies to both the ITSEF and the certification body, but under CSA Art. 60(1)/Annex as the base layer, with IR 2024/482 Arts. 21–22 adding EUCC-specific conditions (and Arts. 23–24 governing the notification of each).

7.2 Standards for Accreditation for Notification

These standards are **ISO/IEC 17025 for ITSEFs**, as per the ENISA SotA document[16], complemented by **ISO/IEC TS 23532-1** and the applicable EUCC-specific requirements.

The scope of the ITSEF accreditation covers the relevant Common Criteria/Common Evaluation Methodology evaluation activities for which the ITSEF has demonstrated competence. The requirements for the competence of personnel in **ISO/IEC 19896-1:2025** and **ISO/IEC 19896-3:2025** are relevant to ITSEF evaluators and to certification-body personnel reviewing evaluations performed under ISO/IEC 15408 and ISO/IEC 18045. They may also be used for personnel in CRA notified bodies where those evaluation methodologies form part of the CRA assessment, but they do not replace the applicable standard for organisational accreditation.

NOTE: This is a transitional arrangement. Under EA TMB Resolution 2022 (09) 01, ISO/IEC 17065 is considered the most suitable accreditation standard for bodies performing evaluations, on-site audits and surveillance under the EUCC scheme. However, recognising that these activities have historically been performed by ITSEFs under ISO/IEC 17025 and accepted under the CCRA and SOGIS-MRA Mutual Recognition Arrangements, the TMB accepts their continued performance under ISO/IEC 17025. ENISA has been asked to transition activities that do not fit within ISO/IEC 17025 to certification bodies accredited to ISO/IEC 17065, with a recommended transition period of five years.

EN ISO/IEC 17065 governs **CBs**, per the ENISA SotA document[17], in their EUCC certification functions, including reviews of ITSEF evaluation results and technical reports and the associated certification decisions and certificate lifecycles. The applicable EUCC-specific requirements are further specified in the relevant ENISA SotA documentation.

7.3 Competence Requirements for EUCC CABs (CBs and ITSEFs)

The tables below list the competence requirements for EUCC CABs – certification bodies and ITSEFs – related to the scope of accreditation, organised under the three categories of requirements introduced in Section 3. Under the CSA, these are CABs notified pursuant to Article 61; 'notified body' is reserved in this report for the NLF/CRA and RED contexts. Section 7.4 details the competence requirements related to the type of conformity assessment activity.

Table 12. EUCC: Specific requirements related to the scope of accreditation

AREA OF COMPETENCE	REQUIREMENTS	STANDARD REFERENCES
Product-specific conformity assessment capability	As per the ENISA SotA on ITSEF accreditation (Annex A), ITSEF competence is additionally scoped by technology type and evaluation-technique type. At the 'substantial' level, the following domains apply. **Technology types.** Hardware and software architectures, operating systems, application security; network and wireless; secure microcontrollers and smartcards; cryptography. **Evaluation-technique types.** Source code review; cryptographic analysis; vulnerability analysis and penetration testing (generic); vulnerability analysis and penetration testing (smartcards); vulnerability analysis and penetration testing (hardware security boxes).	ENISA SotA on CB accreditation (Annex – Technology and evaluation technique types); ENISA SotA on ITSEF accreditation (Annex A). Applicable to CB and ITSEF.

Table 13. EUCC: Specific requirements related to the type of conformity assessment activity

AREA OF COMPETENCE	REQUIREMENTS	STANDARD REFERENCES
Competence to perform IT security testing	Security Target Evaluation (ASE); Design & Architecture Review (ADV); Guidance Review (AGD); Lifecycle & Process Assessment (ALC); Functional Security Testing (ATE); Vulnerability Analysis & Penetration Testing (AVA); Cryptographic Assessment; Patch Management Assessment; Compliance Mapping & Certification Review	ISO/IEC 19896-1 and -3:2025; ISO/IEC TS 23532-1:2021; ITSEF evaluators and CB reviewers, as applicable
Competence to execute testing activities in a competent, independent, and reproducible manner	Technical and methodological competence: method verification and validation, statistical proficiency. Metrological and evaluative competence: traceability, measurement of uncertainty. Management of deviations and nonconformities. Operational and information control	ISO/IEC 17025:2017, clauses 6.1–6.5, 7.1–7.8, 7.10–7.11 (ITSEF). Applicable to ITSEF
Capability to examine the manufacturer's vulnerability-handling processes	Partially covered by the Lifecycle & Process Assessment (ALC) and Patch Management Assessment activities	ISO/IEC 19896-1 and -3:2025; ISO/IEC TS 23532-1:2021. EUCC activities only; not full CRA Annex I, Part II competence
Outsourced capabilities	Subcontracting requirements as per the standard	ISO/IEC 17065:2012, clause 6.2.2. Applicable to CBs

Section 7.4 below sets out the full breakdown of requirements.

7.4 Competence Requirements by Conformity Assessment Activity

This section sets out the testing and evaluation activities that define the technical competence required of an ITSEF and a CB performing conformity assessment under the EUCC scheme at the **'substantial'** assurance level. Activities are derived from the ISO/IEC 15408:2022 Security Assurance Requirements and the ISO/IEC 18045:2022 evaluation methodology (CEM), as interpreted by the ENISA state-of-the-art documents on ITSEF and CB accreditation (v1.6, November 2024).

The substantial level maps to AVA_VAN.1 (EAL1) and AVA_VAN.2 (EAL2–EAL3). Each activity corresponds to a defined set of CEM evaluator work units with deterministic pass/fail criteria. The identifiers marked **[Proposed extended component]** are taken from the ENISA study *Cyber Resilience Act implementation via EUCC and its applicable technical elements* (January 2025). The study expressly states that these components do not exist in the current ISO/IEC 15408-2 or ISO/IEC 15408-3 catalogues. They are proposed analytical mappings intended to identify CC technical elements that could cover CRA requirements. The study does not provide complete definitions of components or dependencies for each proposal and characterises the mappings as preliminary. Accordingly, identifiers such as ADV_ARC.2, ADV_PDM.1, AGD_DEC.1, ALC_FLR.4, ALC_SBM.1 and ALC_PSR.1 are used in this report only as proposed analytical constructs. They could not be used as formal EUCC requirements unless complete extended definitions of components were prepared and evaluated in accordance with the extension rules in ISO/IEC 15408.

Determination methods. An ITSEF and a CB jointly determine conformity by:

1. The **ITSEF examining the developer's evidence** (the Security Target, design and architecture documentation, guidance documentation, and lifecycle and configuration-management documentation) against the assurance components claimed in the Security Target, to verify that each CEM work unit prescribed by ISO/IEC 18045 is satisfied (ASE, ADV, AGD, ALC);
2. The **ITSEF independently devising and executing functional tests** on a sample of the TOE's security functionality (ATE_IND), including, where required, repeating a sample of the developer's own tests, to verify the TOE behaves as documented;
3. The **ITSEF conducting independent vulnerability analysis and penetration testing** (AVA_VAN) – surveying public-domain sources, generating vulnerability hypotheses and executing penetration tests at the assurance level's defined attack potential – to determine whether exploitable residual vulnerabilities remain;
4. The **ITSEF assigning a pass/fail/inconclusive verdict** to each CEM work unit, aggregating these into assurance-component verdicts and documenting all findings in the Evaluation Technical Report (ETR);
5. The CB reviewing the ETR and the underlying evaluation evidence, confirming the verdicts, and issuing the certification decision and EUCC certificate at the assurance level achieved (AVA_VAN.1 or AVA_VAN.2 for 'substantial').

NOTE: Unlike CRA and RED, where a single NB carries out both the technical assessment and the conformity decision, EUCC splits these roles structurally: the ITSEF performs the evaluation (steps 1–4), and the CB performs the independent review and decision (step 5). Section 7.5 sets out how this split maps onto the CRA-Module B notified-body model.

7.4.1 Security Target evaluation (ASE)

This evaluation comprises a review of the Security Target (ST) – the document defining the product's boundary and security claims – for internal consistency, completeness and technical soundness.

- **An ST-introduction review** (ASE_INT.1) verifies a unique TOE reference, an overview of usage and major security features, and a description covering the physical and logical scopes.
- **A Security-problem definition review** (ASE_SPD.1) examines documented threats, organisational security policies, and environmental assumptions for completeness and internal consistency.

- **A Security-objectives review** (ASE_OBJ.1/2) verifies that objectives are defined, traced to the security problem and are sufficient to address all threats and policies.
- **A Security-requirements review** (ASE_REQ.1/2) verifies that SFRs and SARs are correctly stated and internally consistent, and that the SFR rationale demonstrates that all threats are countered.
- **A TSS review** (ASE_TSS.1) verifies the TOE Summary Specification and describes how each SFR is met, at a level that enables the reader to understand how the TOE satisfies its requirements.
- **A Conformance claims review** (ASE_CCL.1) verifies the claimed conformance to the CC version, packages and protection profiles.

7.4.2 Design and architecture review (ADV)

- **A Functional-specification review** (ADV_FSP.1/2) verifies that all TSF interfaces are identified and described with purpose, method of use, parameters and security-relevant behaviour.
- **A Security-architecture review** (ADV_ARC.1) confirms that the TSF protects itself from tampering, cannot be bypassed, enforces domain separation and initialises securely.
- **A TOE-design review** (ADV_TDS.1/2) verifies the design documentation that describes the TOE's subsystems and interactions and identifies SFR-enforcing subsystems.
- **A Secure default configuration review** (ADV_ARC.2, [Proposed extended component]) assesses that the TOE enforces a secure configuration as delivered, prior to any user configuration and examines the developer's rationale for the default state.
- **A Data minimisation review** (ADV_PDM.1, [Proposed extended component]) verifies the developer's rationale for data minimisation to see that all user data processed by the TOE is identified, related to input/output interfaces, and justified as necessary and adequate.

7.4.3 Guidance review (AGD)

- **A Preparative-guidance review** (AGD_PRE.1) verifies that procedures describe all steps for secure acceptance and installation, including how the user can verify they received the correct, unmodified product.
- **An Operational-guidance review** (AGD_OPE.1) verifies that guidance describes all user-accessible functions, security-relevant events, configuration warnings and instructions for secure operations across all user roles.
- **A Decommissioning-guidance review** (AGD_DEC.1, [Proposed extended component]) verifies that decommissioning procedures describe complete end-of-life disposal steps, required tools, effectiveness at precluding access to protected assets and compatibility with the operational environment.

7.4.4 Lifecycle and process assessment (ALC)

- **A Configuration-management review** (ALC_CMS.2) verifies that a configuration item list exists, uniquely identifying the TOE, its parts, evaluation evidence and flaw reports.
- **A Delivery-procedures review** (ALC_DEL.1) verifies that procedures maintaining TOE security during distribution have been documented and applied.
- **A Lifecycle-definition review** (ALC_LCD.1) verifies that the developer documents a lifecycle model for development, production and maintenance with a justification of adequacy.
- **A Flaw-remediation review** (ALC_FLR.1/2/3) verifies procedures for tracking, describing and correcting security flaws. FLR.2 contains additional guidance on user-facing reporting. FLR.3 discusses timely responses and the automatic distribution of corrections.
- **A Flaw-separation review** (ALC_FLR.4, [Proposed extended component]) verifies that corrections of security flaws are distributed separately from corrections of functional flaws.

- **A SBOM verification** (ALC_SBM.1, [Proposed extended component]) verifies that the developer provides a Software Bill of Materials in machine-readable format (CycloneDX 1.4 or higher or SPDX 2.3 or higher or ISO/IEC 5962:2021 per ENISA guidance), listing minimally all top-level third-party components with name, version, developer URI, licence and hash.
- **A Periodic-security-review verification** (ALC_PSR.1, [Proposed extended component]) verifies that the developer maintains procedures for periodic security review and testing of the TOE, at least annually for at least five years post-evaluation, with evidence of exercise.

7.4.5 Functional security testing (ATE)

- **A Developer functional test review** (ATE_FUN.1) verifies the developer produced and executed a test plan covering all SFR-described security functionality.
- **A Test-depth verification** (ATE_DPT.1) verifies that the developer's testing demonstrates the correct operation of all TSF subsystems, with sufficient design-abstraction coverage.
- **In an Independent-evaluator testing** (ATE_IND.1/2) the evaluator independently devises and executes tests on a sample of security functions, and at IND.2, also independently repeats a sample of the developer's own tests.

7.4.6 Vulnerability analysis and penetration testing (AVA)

This is an adversarial analysis to identify and determine the exploitability of potential vulnerabilities, at a basic attack potential (AVA_VAN.1 public-source survey, or AVA_VAN.2 with additional TOE information).

- **A Public-domain vulnerability survey** is a systematic search of vulnerability databases, advisories and academic/conference sources for potential TOE vulnerabilities.
- **A Vulnerability-hypothesis generation** is the generation of a list of potential vulnerabilities exploitable in the operational environment, based on the survey and available documentation.
- **A Penetration-test planning and execution** is the development and execution of test cases against the operational TOE, assuming a basic attack potential (limited time, lay-to-proficient expertise, public knowledge, standard equipment).
- **An Attack-potential assessment** is the calculation per the CEM framework (elapsed time, expertise, knowledge, opportunity, equipment) of the attack potential required for exploitation.
- **A Residual-vulnerability determination** is a determination of whether exploitable residual vulnerabilities remain within the defined attack potential, documented in the evaluation technical report.

7.4.7 Cryptographic assessment

- **A Cryptographic-operation verification** (FCS_COP.1) confirms the correct implementation of documented algorithms, key sizes and modes against applicable EUCC/ENISA state-of-the-art documents and recognised cryptographic catalogues, including NIST SP 800-series references where relevant.
- **A Key-generation, derivation, and destruction assessment** (FCS_CKM.1/5/6) verifies that key generation (including RNG source), derivation and destruction conform to documented methods and referenced standards, with no residual key material after destruction.
- **A Random-number-generation assessment** (FCS_RNG.1) verifies that the RNG produces output with sufficient entropy for the security-strength claims it supports.

7.4.8 Patch management assessment

This is an assessment of the technical mechanisms and procedures for the secure distribution of updates, as per EUCC Implementing Regulation (EU) 2024/482, Article 25.

- **Patch-mechanism functional testing** verifies the TOE implements secure update authentication, integrity verification and the correct application of patches.
- **Automatic-update default and notification testing** ([CRA-specific augmentation]) verifies, where applicable, that automatic updates are enabled by default within an appropriate timeframe, with an opt-out mechanism and user notification with a postponement option.
- **A Patch-policy review** verifies that the developer's patch management policy addresses timely responses to vulnerabilities, the separation of security from functional updates, and the distribution of patches to affected users.

7.4.9 Compliance mapping and certification review

This is an assessment of the cross-cutting activities that aggregate evaluation results into the certification decisions. The CB reviews the ITSEF's work and issues the conformity verdict.

- **Evaluation-technical report production.** The ITSEF documents all findings, verdicts and justifications for the evaluation of each component of the assurance.
- **CB review of evaluation results.** The CB verifies the completeness, consistency and correct application of the methodology and ensures that all verdicts are supported by evidence.
- **Certificate-scope determination.** This is a determination of the precise scope of the certificate. It covers the identification of the TOE, the evaluated configuration, assurance level and any augmentations.
- **CRA conformance-claim template** ([CRA-specific augmentation]). This template is used where the EUCC certificate supports a CRA declaration of conformity and the completion of the template mapping of SFRs/SARs to the applicable essential requirements of the CRA, with rationales for non-applicability referenced to the SPD.
- **Protection-Profile conformance verification.** Where the ST claims PP conformance, this verification confirms that all PP requirements are met (strict, demonstrable or exactly as claimed).

7.4.10 Technology-specific competence areas

According to the ENISA SotA on ITSEF accreditation (Annex A), ITSEF competence is additionally scoped by type of technology and type of evaluation technique. The accreditation assessment report must detail in which one of these types the ITSEF has demonstrated competence.

Technology types:

- **Hardware and software architectures, operating systems, application security.** These are processor architectures, OS security models, sandboxing, memory protection and privilege separation.
- **Network and wireless.** These are network protocols, wireless communication security, protocol-stack vulnerabilities and network-level attack vectors.
- **Secure microcontrollers and smartcards.** These are smartcard architectures, side-channel resistance, HSMs, embedded security mechanisms. *Primarily relevant to EUCC 'high' level but may apply at the 'substantial' level for specific product categories.*
- **Cryptography.** This covers algorithm design, implementation security, key management and reference catalogues sufficient to evaluate FCS-class SFRs.

Evaluation technique types:

- **Source code review.** An examination of evidence of implementation for vulnerabilities and secure-coding properties, using the ENISA EUCC SotA *Accreditation of ITSEFs for the EUCC Scheme* technique in Annex A.2.1. Its inclusion depends on the evaluation requirements, available evidence and the ITSEF's demonstrated competence and scope. ADV_IMP is not part of the usual EAL1–EAL3 baseline; however, the EUCC assurance label alone does not

determine whether source-code evidence can be examined. Any additional CRA assessment must have the necessary evidence of access, methods and competence.

- **Cryptographic analysis.** An assessment of algorithm correctness, key management soundness, RNG quality and protocol-level security.
- **Vulnerability analysis and penetration testing (generic).** Public-domain surveys, the generation of hypotheses, the planning and execution of penetration tests, and the calculation of attack potentials using the CEM. It is applicable to software and generic IT products.
- **Vulnerability analysis and penetration testing (smartcards).** The physical and logical attack techniques specific to smartcards, i.e. side-channel analysis, fault injection and hardware probing. *Primarily relevant at the 'high' assurance level.*
- **Vulnerability analysis and penetration testing (hardware security boxes).** The physical attack techniques for hardware devices with security enclosures, i.e. tamper detection, environmental attack testing and physical penetration. *Primarily relevant at the 'high' level.*

7.5 EUCC – CRA Module B Gap Analysis and Competence Comparison

EUCC CBs accredited under ISO/IEC 17065 have a strong organisational and certification-system foundation relevant to CRA Module B. However, EUCC accreditation does not automatically demonstrate compliance with the CRA. The certification body must adapt its procedures and documentation to the CRA context, demonstrate compliance with CRA Article 39 and extend its accreditation and scope of notification to the relevant CRA Module B activities and product families.

The IT security evaluation and testing competences required for EUCC ITSEF accreditation provide a substantial foundation for the activities described in CRA Annex VIII, Part II, point 4.1, i.e. to *examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I.* However, the extent of the overlap depends on the ITSEF's accredited Common Criteria assurance components, technical domains, product categories and evaluation techniques. Additional CRA-specific competence may therefore be required.

EUCC ITSEF accreditation also provides a relevant but incomplete foundation for competence for assessing the vulnerability handling processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I. Depending on the accredited scope, this may include the remediation of ALC flaws and the evaluation of lifecycle support, vulnerability monitoring, product reassessment and certain audit activities. However, **ITSEF accreditation does not automatically demonstrate competence** to assess the complete CRA Annex I, Part II vulnerability-handling framework or conduct the CRA-specific periodic audits required by Annex VIII, Part II, point 8.

The CAB must therefore demonstrate the additional competences in process inspection as required for the CRA, including fulfilment of the relevant ISO/IEC 17020 provisions on competence (clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10). This does not require separate ISO/IEC 17020 accreditation.

Accordingly, the gap is **an extension of an existing ITSEF competence base**, not a new inspection function. The exact gap must be determined from the individual ITSEF's scope of accreditation, including the assurance levels at which it evaluates.

ITSEFs also do not, on their own, fulfil the impartiality, independence and consistent-operation requirements that ISO/IEC 17065 defines for a notified body. Where the CB and ITSEF are separate bodies – or separate units within the same legal entity – the CRA notified body remains responsible for the complete Module B procedure and final certification decision.

The following table of comparison identifies how the relevant requirements for CRA competence are addressed by the existing EUCC CB and ITSEF frameworks.

Table 14. EUCC – CRA Module B: Competence and Accreditation Mapping

AREA OF COMPETENCE / REQUIREMENT	CRA REFERENCE REQUIREMENTS	EUCC CB	EUCC ITSEF
Scope-specific competence			
Assessment of technical design and development within the product category/family within the scope	(Annex – Technology and evaluation technique types)	(Annex – Technology and evaluation technique types)	(Annex – Technology and evaluation technique types)
Conformity-assessment activity competence			
IT security testing	CRA Annex I, Part I	**Not applicable**	ENISA SotA on ITSEF accreditation, Annex A
Competent, independent and reproducible execution of testing activities	ISO/IEC 17025:2017, Clauses 6.1–6.5, 7.1–7.8 and 7.10–7.11	**Not applicable**	ISO/IEC 17025:2017, Clauses 6.1–6.5, 7.1–7.8 and 7.10–7.11
Examination of manufacturer vulnerability-handling processes	EA-2/17 S1 M:2026, Table 1 and Key '*pk*', referencing EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; ISO/IEC 30111:2019; ISO/IEC 29147:2018.	**Review and control of applicable EUCC lifecycle evaluation results**; complete CRA process coverage and periodic auditing must be demonstrated separately.	**Partial foundation** through relevant ALC_FLR and other ALC components, subject to the accredited scope. It does not establish coverage of the complete CRA Annex I, Part II framework or Module B periodic audits.
Outsourced conformity-assessment activities	ISO/IEC 17065:2012, Clause 6.2.2	ISO/IEC 17025:2017, Clause 7.9	ISO/IEC 17065:2012, Clause 6.2.2
Structural and process requirements			
General requirements	ISO/IEC 17065:2012, Clause 4	ISO/IEC 17065:2012, Clause 4	**Not applicable**
Structural requirements	ISO/IEC 17065:2012, Clause 5	ISO/IEC 17065:2012, Clause 5	**Not applicable**
Process requirements	ISO/IEC 17065:2012, Clause 7	ISO/IEC 17065:2012, Clause 7	**Not applicable**
Management system requirements	ISO/IEC 17065:2012, Clauses 8.2–8.8; ISO 9001:2015	ISO/IEC 17065:2012, Clauses 8.2–8.8; ISO 9001:2015	**Not applicable**

Section 7.6 below sets out the full comparative analysis and the skills-development programme needed to close the identified gaps in competence.

7.6 IT Security Assessment Capability Gap Analysis: CRA and EUCC

This section examines whether an ITSEF accredited for EUCC evaluations at the 'substantial' assurance level has the technical qualifications relevant to CRA conformity assessment. The analysis distinguishes Security Functional Requirements from ISO/IEC 15408-2, Security Assurance Requirements from ISO/IEC 15408-3 and proposed extended components from the ENISA study *Cyber Resilience Act implementation via EUCC and its applicable technical elements* (January 2025). The proposed components are not current EUCC requirements. The comparison addresses whether ITSEF personnel possess the skills, tools and domain knowledge needed for the corresponding activities.

Two scenarios must be distinguished: a) an EUCC-accredited CB or ITSEF being notified as a CRA Module B body, where the notified body must assess all applicable Annex I requirements, including requirements for which the EUCC scheme provides no bridge, and b) a EUCC certificate used to show CRA conformity (Art. 27(8)-(9); Art. 8(1) for Annex IV products where the applicable legal conditions are met). The latter does not reduce the competence or coverage required of a body notified to perform the complete Module B procedure.

The same qualitative gap levels defined in Section 2.1 are used as follows.

- **None.** Existing CC evaluation of competence directly covers the requirement and no additional training, tooling or expertise is needed.
- **Low.** The requirement extends an existing CC competence, so a modest investment in training or familiarisation is sufficient.
- **Medium.** The requirement involves a materially new domain of knowledge or evaluator judgement with no CEM precedent; thus training, guidance and scheme-level harmonisation are needed.
- **High.** The requirement involves skills, tools or expertise fundamentally outside the CC evaluation paradigm.

These ratings are qualitative desk-based estimates for capacity planning that draw on stakeholder feedback. They are not measurements of efforts in implementation, a validated sector-wide benchmark or a determination on accreditation or notification. NABs, NCCAs and CABs should validate their applicability against the individual body's personnel, methods, access to evidence, technology coverage and scope of assessment.

7.6.1 Requirement-by-Requirement Bridge and Gap Assessment

Table 15. CRA–EUCC Mapping of CAB Technical Competence Requirements and Qualification Gaps

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
Risk-based cybersecurity design (ESR 1)	ASE_SPD.1, ASE_OBJ.1 and ASE_REQ.1 provide a methodological bridge for assessing the documented security problem,	**Partial foundation**. ITSEF personnel assess threats, assumptions, organisational security policies and their traceability to security objectives and	**Material extension**. Evaluators require knowledge of cybersecurity risk-assessment methodologies sufficient to assess whether the	**Medium**

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
	security objectives and requirements rationale. They do not provide a direct equivalent to assessment of the manufacturer's complete product-level cybersecurity risk assessment.	requirements. The risk analysis underlying the Security Problem Definition is ordinarily outside the CC evaluation.	manufacturer's product-level assessment is sound, complete and appropriate across the complete product lifecycle. The CRA does not prescribe a specific methodology, and the CAB assesses rather than performs the manufacturer's risk assessment.	
Vulnerability-free product (ESR 2a)	**AVA_VAN.1/2** – vulnerability analysis, including public-domain vulnerability research and penetration testing at the applicable attack potential.	**Established**. EUCC ITSEFs have competence in vulnerability analysis, vulnerability hypothesis generation and penetration testing in accordance with CC/CEM.	EUCC ITSEFs have an established vulnerability-analysis and penetration-testing foundation. However, the depth required for CRA assessment depends on the product category, identified risks and applicable technical specifications. Evaluation at basic attack potential cannot automatically be considered sufficient, particularly for important class II or critical products. **No additional competence gap** arises where the required methods and depth are already covered by the ITSEF's demonstrated competence and scope. **Otherwise, additional** methods, tools, specialist expertise or scope extension may be needed.	**None** where the required assessment depth is already covered; **otherwise,** scope-dependent
Secure-by-default configuration (ESR 2b)	**ADV_ARC.2** (Proposed extended component) – assessment of the secure-default rationale. Existing ADV_ARC.1 security-architecture assessment and	**Partially established** – through assessment of secure initialisation, self-protection, non-bypassability and domain separation. ADV_ARC.2 extends this with one additional work unit assessing default	**Limited extension** – Requires the evaluator to assess the default exposure of interfaces, protocols, services and settings, and the completeness of the developer's rationale. Requires familiarity with	**Low**

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
	applicable FMT requirements provide a partial methodological foundation; the secure-as-delivered configuration must be assessed explicitly.	configuration state, but it is not a current catalogue component.	product-specific default states (e.g., which ports are open, which services are running out-of-the-box). Training on the extended component and its application across diverse product types is needed. ADV_ARC.2 is an analytical reference rather than an existing EUCC requirement	
Secure updates with automatic defaults, opt-out, notification and postponement (ESR 2c)	**SFRs per EUCC Patch Mechanism** (ENISA study proposes ISO/TS 9569 as reference). The mechanism must include auto-update default, opt-out, user notification, postponement option.	**Partially established –** ITSEFs have competence in ALC_FLR family evaluation. The EUCC patch mechanism is established but its SARs are not yet fully specified with CEM-level work units. Evaluators have general experience testing update functions.	**Limited extension** – The four CRA-specific constraints (auto-default, opt-out, notification, postponement) go beyond what any standard CC SAR requires. The ITSEF needs guidance on how to test each constraint as a distinct functional property. The underlying competence (functional testing of management interfaces) exists, but the specific test criteria for these four properties require new scheme-level guidance.	**Low**
Access control, authentication and security event reporting (ESR 2d)	**FIA, FDP, FMT and FAU SFRs** provide established CC mechanisms for identification and authentication, access control, security management and audit.	**Established** – these SFR classes are among the most commonly evaluated in CC. Evaluators have deep operational experience with these SFRs across diverse products.	**None** – the required capabilities are well covered by existing CC/CEM evaluation competence.	**None**
Data confidentiality at rest and in transit (ESR 2e)	**FDP_SDC.1, FCS_COP.1, FTP_ITC.1 and FTP_TRP.1** – cover protection of stored data, cryptographic operations and	**Established** – ITSEFs routinely evaluate FCS and FTP requirements; Cryptographic assessment is a defined technique type per ENISA SotA Annex A.2.2,	**None** for the evaluation itself. The ENISA study notes the FCS dependency chain is complex (key generation, derivation, destruction, RNG) but this is standard CC practice for ITSEFs	**None**

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
	trusted channels/paths.	requiring specific accredited competence.	with cryptographic analysis accreditation.	
Data integrity at rest and in transit, including corruption reporting (ESR 2f)	**FDP_SDI.1/2, FTP_ITC.1, FTP_TRP.1 and FAU_GEN.1** for corruption reporting.	**Established** – Core ITSEF competence. FDP_SDI and FAU_GEN are commonly evaluated.	**None**	**None**
Data minimisation (ESR 2g)	**ADV_PDM.1** (Proposed extended component) – Rationale-based assessment of whether processing is adequate, relevant and necessary.	**Partial analytical foundation** in interface and data-flow analysis. Competence to judge necessity and adequacy of processing cannot be presumed from CC evaluation experience alone.	**Additional** data-protection knowledge and necessity-based evaluator judgement are required. Existing interface and data-flow analysis provides a related foundation, but competence to assess the complete CRA data-minimisation requirement must be demonstrated separately. This requires training in data protection concepts and scheme-level guidance on what constitutes “necessary” across product categories. Without such guidance, evaluator judgement will diverge significantly.	**Medium**
Availability / DoS resilience (ESR 2h)	**Study mapping: FRU_FLT.1 and FPT_FLS.1**. FRU_RSA.1/2[18] are Common Criteria (ISO/IEC 15408) security functional requirements designed to prevent denial-of-service (DoS) attacks caused by resource monopolization. Fault-tolerance and secure-state	**Relevant foundation** where the ITSEF’s scope includes resource-management, availability or fault-tolerance evaluation. Competence must be demonstrated through relevant evaluation and testing experience.	**Extend existing competence** to define and execute product-specific DoS and resource-exhaustion tests, including load or traffic generation where appropriate. Confirm coverage of the applicable CRA availability requirement beyond the selected CC components. ITSEFs with relevant experience may already possess the	**Low–Medium**

[18] FRU_RSA.1/2 reference is an analytical refinement based on CC:2022, Part 2, §16.4, additional to the ENISA study’s original mapping

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
	evaluation provide complementary coverage. Coverage depends on the requirements selected in the ST/PP and the supporting tests; it does not automatically establish complete CRA DoS resilience		methods and tools; others need dedicated training and equipment.	
Minimise negative impact on other devices/networks (ESR 2i)	**FPT_INI.1, FPT_TST.1** – secure initialisation, integrity and self-testing; FDP_IFC.1/IFF.1 where network traffic control applies.	**Established** – FPT_INI and FPT_TST are known SFRs. Evaluation of boot integrity and self-test is standard at higher EALs but less common at substantial. Traffic filtering SFRs are familiar from firewall/IDS evaluations.	**Limited scope-dependent gap** – For products that do not control network traffic, ITSEF tests boot integrity and self-test functions. For network equipment requiring FDP_IFC/IFF evaluation, the ITSEF needs competence in network security testing (traffic analysis, rule verification). This is covered by ENISA SotA technology type “Network & wireless” but must be within the ITSEF’s accredited scope.	**Low**
Limit attack surfaces, including external interfaces (ESR 2j)	**AVA_VAN.1, ADV_FSP.1 and AGD_OPE.1** – identification of interfaces through the functional specification and guidance, followed by vulnerability analysis of those interfaces.	**Established** – interface identification and vulnerability analysis are standard CC/CEM evaluation activities.	**None** – the EUCC evaluation framework provides the relevant competence. Greater analysis of implementation-level attack surface may affect evaluation depth, but does not constitute an additional qualification requirement.	**None**[19]
Exploitation mitigation and	**FPT_FLS.1, FPT_RCV.1 and ADV_ARC.1** – secure-state	**Established** – ITSEFs have competence in evaluating FPT and ADV_ARC requirements,	**None within the defined scope** – the EUCC–CRA bridge does not require binary-level verification of	**None**[20]

[19] Limited interface- or architecture-level assessment. Additional source-code or implementation-level assessment is considered separately; the rating does not imply complete coverage of the corresponding CRA requirement
[20] Limited interface- or architecture-level assessment. Additional source-code or implementation-level assessment is considered separately; the rating does not imply complete coverage of the corresponding CRA requirement

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
secure recovery (ESR 2k)	preservation, recovery mechanisms and supporting security architecture.	including secure failure states and recovery mechanisms.	implementation-specific mitigations. Any limitation in assessing such mitigations at the substantial level is an assurance-depth issue, not a qualification gap.	
Security event logging with opt-out (ESR 2l)	**FAU_GEN.1, FMT_SMF.1, FMT_MOF.1 and FMT_SMR.1** – security event generation and management of the audit function, including controlled disabling and role-based access.	**Established** – ITSEFs routinely evaluate FAU and FMT requirements, including audit generation and security-management functions.	**None** – the opt-out mechanism can be assessed as a standard security-management function within existing CC/CEM competence.	**None**
Permanent data removal and secure transfer (ESR 2m)	**Study mapping: FMT_SMF.1, FDP_RIP.1, FDP_ETC.1/2 and FTP_ITC.1** – FDP_RIP.1 protects residual information on resource allocation or deallocation; it does not itself specify user-controlled permanent deletion. The other components provide related management, export and trusted-channel elements. Explicit deletion and secure-transfer requirements and tests are still needed.	**Relevant foundation where the ITSEF has demonstrated** FDP, FMT and FTP evaluation competence, particularly in deletion, export and trusted-channel mechanisms. The evaluated ST/PP determines which functions and data are covered; **residual-information protection alone does not establish complete CRA coverage**.	**Limited extension** – verify explicit coverage of user-controlled permanent removal of the required data and settings, and secure transfer where that functionality is provided. Assess operation and effectiveness using product-appropriate tests, including data-recovery attempts where warranted. Assumes relevant deletion and transfer competence is already demonstrated.	**Low**
Vulnerability identification, SBOM (Part II, ESR 1)	ALC_SBM.1 (Proposed extended component) – Machine-readable (CycloneDX/SPDX format) SBOM verification. **ALC_FLR components** support	**Partially established** – ITSEFs have established competence, through component analysis and flaw-remediation evaluation, depending on their actual scope and experience.	**Limited extension** – additional competence is needed to assess machine-readable SBOMs and verify their completeness and consistency against the TOE. Familiarisation with	**Medium**

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
	flaw tracking and remediation but do not establish complete CRA SBOM verification.		relevant formats and tools may be required.	
Timely remediation and secure update distribution (Part II, ESR 2/7/8)	**ALC_FLR.3 or ALC_FLR.1 and EUCC patch management** arrangements provide related evidence**; ALC_FLR.4** (Proposed extended component) addresses separation of security and functional updates. The complete applicable CRA requirements must still be assessed	**Established / partially established** – Relevant flaw-remediation, update-management and functional-testing experience may provide a foundation, subject to the actual evaluation scope.	**Limited extension** of demonstrated update and flaw-remediation competence to the applicable CRA technical properties. The complete periodic process-audit function is assessed separately. Whether updates are provided free of charge is a manufacturer obligation assessed on non-technical grounds, not an additional notified-body assessment activity or competence requirement	**Low**
Regular security testing (Part II, ESR 3)	**ALC_PSR.1** (Proposed extended component) – assessment of manufacturer's regular security-testing programme. Relevant ALC evidence provides a partial basis but does not establish complete CRA coverage.	**Partially established** – ITSEFs have partial foundation in reviewing developer procedures and security-testing evidence. The scope of the ongoing programme must be assessed separately.	**New competence element** – Evaluators need sufficient security-testing knowledge and process-assessment judgement to assess the programme's coverage, implementation and adequacy.	**Medium**
Vulnerability disclosure, sharing and contact address (Part II, ESR 4/5/6)	**ALC_FLR.2** – flaw reporting procedures; EUCC Article 8(6)(b) provides a related CVD requirement.	**Partially established** – ALC_FLR.2 supports flaw-reporting and communication assessment but does not automatically establish coverage of all CRA Part II(4)–(6) requirements or their continuing implementation.	**None** – the required assessment capabilities are already covered by existing EUCC competence.	**None**
Secure decommissionin	**AGD_DEC.1** (Proposed extended	**Partially established** – ITSEFs have established	**New competence element** – evaluators	**Medium**

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE (PER ENISA STUDY)	EXISTING ITSEF COMPETENCE	QUALIFICATION GAP	GAP LEVEL
g guidance (CRA Annex II, Requirement 8(d))	component) – assessment of decommissioning procedures, including completeness, tool specification, effectiveness and environmental considerations.	AGD competence (AGD_PRE, AGD_OPE), but decommissioning extends this to end-of-life, an additional lifecycle phase.	require additional knowledge to assess whether data-destruction methods are adequate for the relevant storage technology and use case that goes beyond standard CC guidance review.	

7.6.2 CRA Areas With No EUCC Bridge at Substantial Level

This document explicitly acknowledges CRA requirements that cannot be fully met through EUCC technical elements at the 'substantial' assurance level. Where a CB/ITSEF arrangement seeks CRA Module B notification, these requirements remain within the notified body's scope of assessment and must be addressed according to their nature.

Table 16: CRA Areas With No EUCC Bridge at Substantial Level

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE	EXISTING EUCC COMPETENCE	GAP / LIMITATION	ASSESSMENT
Incident reporting to CSIRTs within 24 h (CRA Art. 14)	**No EUCC equivalent.** No CC SFR/SAR is proposed.	**Not applicable.**	This is an operational manufacturer obligation, not an Annex I essential cybersecurity requirement. It is outside the CRA notified body's Module B/H conformity-assessment scope; compliance falls to competent authorities, CSIRTs, market surveillance, not ITSEFs.	**Outside scope**
Free-of-charge security updates (Part II, ESR 8)	**No direct EUCC equivalent.** The ENISA study proposed a manufacturer declaration controlled by the CAB; that proposal is not adopted here as a notified-body assessment requirement.	**Not applicable**	This ESR is addressed by the manufacturer on non-technical grounds, including the applicable exception for tailor-made products in a business-to-business context. The notified body does not assess whether an update is provided free of charge. This is not an additional CAB	**Manufacturer obligation; no additional NB assessment activity**

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE	EXISTING EUCC COMPETENCE	GAP / LIMITATION	ASSESSMENT
			technical competence gap.	
Support-period documentation review (CRA Art. 13(8))	**No direct EUCC equivalent.** ENISA study proposes documentation of the relevant information in the conformance-claim documentation.	**Not applicable**	A manufacturer-declared lifecycle commitment rather than a technical evaluation activity. The CAB reviews the support-period information only insofar as it forms part of the technical documentation, user information or evidence relevant to conformity	**Documentation check; outside Annex I assessment**
Code-level exploitation mitigations (e.g. ASLR, stack canaries, DEP)	**Not covered at substantial level.** Coverage depends on the evaluated requirements, available source code, binaries or build evidence, and the depth of implementation analysis.	**Scope-dependent.** ITSEFs may already have competence in relevant source-code, binary-analysis and implementation-evaluation.	Demonstrate the necessary evidence access, methods and competence, using additional CRA assessment or relevant EUCC evaluation evidence. Higher-assurance EUCC activities may provide evidence where appropriate, but a high-level EUCC certificate is not an automatic prerequisite for CRA Module B.	**Evidence, depth and scope limitation; individual competence gap assessed separately**
Physical fault injection and tamper testing	**Not covered at substantial level.** Coverage depends on the product's physical threat model, required resistance and evaluated attack methods.	ITSEFs with specialist hardware competence may already possess these methods and equipment, often through higher-assurance evaluations. Other ITSEFs may need additional capability	Where justified by the CRA product risks and requirements, use suitably scoped specialist assessment with the necessary equipment and personnel. Relevant EUCC high-level evidence could support this work, but CRA notification does not itself require upgrading an EUCC certificate or authorisation.	**Product-, risk-, method- and scope-dependent**
Verification of harmonised-standard conformity	**No direct CC/EUCC equivalent.** CC evaluation focuses on conformance with the applicable ST/PP, whereas CRA requires verification of application of harmonised	**Partially established.** ITSEFs have relevant conformance-assessment competence, but CRA introduces a broader	**Additional competence required** for verifying correct application of CRA harmonised standards and, particularly, assessing alternative technical solutions where standards are	**Low–Medium**

CRA REQUIREMENT AREA	EUCC–CRA BRIDGE	EXISTING EUCC COMPETENCE	GAP / LIMITATION	ASSESSMENT
	standards or assessment of alternative solutions against the essential requirements.	assessment against harmonised standards (prEN 40000 series, ETSI EN 304 6xx) and essential requirements.	not applied or provide only partial coverage.	
Non-conformity identification and corrective action	**Partially analogous to CC evaluation findings and verdicts.**	**Established.** ITSEFs and CBs routinely identify findings, obtain corrective actions and verify their resolution before a positive evaluation/certification decision.	**None.** CRA formalises the process but does not introduce a fundamentally new competence requirement.	**None**

7.6.3 Qualification Gap Synthesis

For the comparison of technical competence, the same qualitative gap levels used for the RED assessment are applied. The ratings assess the transferable competence of ITSEF personnel and additional qualification needs; they do not determine whether each activity falls within the scope of ISO/IEC 17025 accreditation. In accordance with EA TMB Resolution 2022 (09) 01, non-testing activities – including certain ALC lifecycle and process assessments, the verification of conformity with harmonised-standards, reviews of risk-based designs and risk-assessments, and assessments of data minimisation – may need to be performed or controlled within the ISO/IEC 17065-accredited certification function. Related ITSEF competence should therefore be treated as a technical foundation, not as evidence that the complete CRA assessment activity is already covered by the ITSEF's accreditation.

The identified gaps in competence, gap levels and assessment rationale are summarised in Table 2 (Section 2.2). The detailed analysis supporting these findings is presented in Sections 7.6.1 and 7.6.2.

No additional qualification gap arises for the following activities where the required product coverage, methods and assessment depth are already demonstrated within the CB/ITSEF arrangement. This is limited to those activities and does not establish complete coverage of the corresponding CRA requirements:

- vulnerability analysis and penetration testing, where the depth required by the product category, identified risks and applicable technical specifications is already covered by the ITSEF's demonstrated competence and scope;
- access control and authentication evaluation;
- data confidentiality and integrity, including cryptographic and non-cryptographic mechanisms;
- security logging and audit;
- attack-surface assessment through interface analysis;
- exploitation-mitigation assessment at the architecture level;
- review of the flaw-remediation and disclosure elements already covered by the evaluated ALC components, with the additional CRA process-assessment and periodic-audit gap addressed separately in Table 2 and Table 15;
- non-conformity identification and corrective action, which are established CB/ITSEF practices formalised under the CRA.

The remaining differences must be addressed according to their nature. **Free-of-charge security updates** under Annex I, Part II(8) remain a manufacturer obligation and is assessed by the manufacturer on non-technical grounds. It is not a notified-body conformity-assessment activity or an additional CAB competence gap. Technical requirements such as update-security and vulnerability-handling remain subject to the applicable assessment. The declared support period is reviewed only through the relevant technical documentation and user information. Compliance with Article 14 **operational incident-reporting obligations** falls **outside** the notified body's assessment of Annex I essential cybersecurity requirements. Code-level exploitation-mitigation assessment and physical fault-injection or tamper testing remain product-, risk-, assurance- and scope-dependent.

7.7 EUCC Certificates as Evidence of CRA Conformity

The use of an EUCC certificate as evidence of CRA conformity is legally distinct from the notification of an EUCC-accredited CB or ITSEF to perform CRA Module B. Under CRA Art. 27(8), a product with digital elements certified under a European cybersecurity certification scheme is presumed to conform to the Annex I requirements to the extent the certificate covers them. Under Art. 27(9) the Commission may specify the relevant schemes, assurance levels and CRA requirements through delegated acts removing the manufacturer's obligation to undergo conformity assessment by a third party for the corresponding requirements, under Article 32(2) and (3). These provisions do not confer CRA notified-body status on the issuing certification body or the evaluating ITSEF.

CRA Article 8(1) provides a specific connection for critical products with digital elements listed in Annex IV. It empowers the Commission, by a delegated act, to require certification at an assurance level that is at least 'substantial' under an available European cybersecurity certification scheme covering the relevant categories of Annex IV products. Where no such act has been adopted, Article 32(3) applies. The route to a certificate remains subject to the applicable legal conditions and the requirements actually covered; it does not permit a Module B notified body to leave applicable Annex I requirements unassessed.

A CB or ITSEF seeking CRA notification must separately demonstrate compliance with Article 39 and competence for the requested scope. EUCC accreditation and authorisation can provide relevant supporting evidence, including organisational and technical evidence, but do not replace that assessment. A CRA Module B assessment does not itself issue an EUCC certificate or require the notified body to hold EUCC authorisation.

8 CRA-Module H: CAB Technical Competences

8.1 Scope of Accreditation

Under CRA Module H, the notified body **assesses and approves the manufacturer's quality system** for design, development, production, final product inspection and testing as well as vulnerability handling. It subsequently performs surveillance of the approved quality system to verify that the manufacturer is fulfilling its obligations under that system, including the relevant arrangements for vulnerability handling, security updates and the maintenance of product information throughout the applicable support period (Annex VIII, Part IV, points 2–4).

Module B also includes post-certification periodic audits of vulnerability-handling processes. Module H is broader because surveillance applies to the manufacturer's **complete approved quality system**, through periodic audits and, where appropriate, unexpected visits[21]. Evidence of product design and development is examined as part of the assessment of the manufacturer's quality system; Module H does not provide for a separate design-examination certificate (Annex VIII, Part IV, point 3).

In accordance with EA-2/17 M:2026, Sections 5 – 5.2, the accreditation documentation identifies the reference standard applied in full. For CRA Module H, Supplement 1 identifies EN ISO/IEC 17021-1 with *pk+qa* obligatory requirements. Supplement 2 provides an informative CRA Module H accreditation-scope entry for Class I products. However, as mentioned in the text *examples presented are not to be seen as mandatory*. Consequently, the scope of accreditation should identify the following.

a. **The applicable legislation.** Regulation (EU) 2024/2847, including the notified-body requirements in Article 39, the essential cybersecurity requirements in Annex I, Parts I and II, and the full-quality-assurance procedure in Annex VIII, Part IV.
b. **The conformity assessment procedure.** Annex VIII, Part IV, Module H: conformity based on full quality assurance.
c. **The product categories or families covered.** These must be identified with sufficient precision and, where relevant, linked to the important and critical product categories in CRA Annexes III and IV. The scope may also cover other product families with digital elements for which the CAB has demonstrated competence to perform Module H.
d. **The applicable product characteristics or specifications.** These include the relevant CRA essential cybersecurity requirements, harmonised-product or management-system standards, common specifications and other applicable sectoral or technical documents.

The scope of accreditation should be sufficiently granular to support the requested notification scope. Under CRA Article 42(2), the application must describe the conformity-assessment activities, procedures or modules and the product or products with digital elements concerned and, where available, include an accreditation certificate attesting compliance with Article 39. Article 43(3) requires the notification to provide corresponding details of the scope and an attestation of competence. Once a CRA-specific product classification is established in NANDO, the accreditation scope should be capable of being mapped to that classification. Where notification is not based on accreditation, the evidence provided under Articles 42(3) and 43(4) should contain sufficient scope-specific detail to demonstrate and monitor competence for the requested notification scope.

The role of harmonised standards, common specifications and other technical standards in demonstrating competence for the requested scope is explained in Section 4 (before Table 5).

A CAB notified for CRA Module H must demonstrate the capability to:

[21] Decision No 768/2008/EC, Annex II, Module H (Quality Assurance), Point 4.4.

1. **assess and approve the manufacturer's quality system**, covering the design, manufacture, final product inspection and testing of products with digital elements;
2. **assess whether the quality system's design controls and supporting technical documentation ensure conformity** with the essential cybersecurity requirements in Annex I, Part I;
3. **assess the quality-system arrangements supporting conformity of product design and development** with Annex I, Part I, and the **vulnerability-handling processes** under Part II, with continuing surveillance under Annex VIII, Part IV, point 4; this does not establish a general SDLC requirement; and
4. **perform these activities through an independent, impartial and consistently controlled conformity-assessment process.**

This has direct staffing implications. The CBs auditing personnel should possess the following competences.

- **Management-system auditing competence** consistent with ISO/IEC 17021-1, including competence to audit the quality-system framework used by the manufacturer. This may include ISO 9001, ISO/IEC 27001 or another appropriate framework. The CRA does not prescribe a specific management-system standard.
- **Product- and process-assessment competence** sufficient to make professional judgements on the relevant product requirements. For CRA Module H, EA-2/17 S1 M:2026 specifies *pk*, referring to EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10. Separate ISO/IEC 17020 accreditation is not implied.
- **Legal and regulatory competence**, covering the CRA, applicable essential cybersecurity requirements, relevant harmonised standards and conformity-assessment obligations.
- **Product-design and cybersecurity competence**, covering the relevant technologies, cybersecurity risks, state-of-the-art and the manufacturer's controls for maintaining conformity.
- **Production and lifecycle-assurance competence**, covering mass production, final inspection and testing, vulnerability handling, security updates and other processes maintained throughout the support period.

The CAB's management system must define competence criteria for each certification function. Personnel who are conducting audits and technical assessments, reviewing the results and making certification decisions must be competent in their assigned functions. The certification decision must be made by personnel who were not involved in the audit.

8.2 Standards for Accreditation for Notification

EA-2/17 S1 M:2026 identifies **EN ISO/IEC 17021-1** as the obligatory accreditation standard for CRA Module H, supplemented by *pk* (product-related professional judgement) and *qa* (quality-system assessment and approval). This supports assessment and surveillance of the manufacturer's approved quality system. The 2026 transition arrangements are described in Section 1.2. Accordingly, note the following.

- **ISO/IEC 17021-1:2015** is the overarching standard governing the certification body's management-system audit function, organisational structure and certification decision-making.
- The *pk* requirements in EA-2/17 S1 M:2026 refer to EN **ISO/IEC 17020:2012** clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10. The *qa* requirements address competence to assess and approve the manufacturer's quality system and identify relevant EN **ISO/IEC 17021-1:2015** provisions.
- **ISO 9001:2015** applies as an alternative management-system option (Option B) for the certification body's own management system, in accordance with ISO/IEC 17021-1:2015, clause 10.3. This concerns the CAB and does not prescribe the manufacturer's quality-system framework.

The manufacturer's quality system is assessed against CRA Annex VIII, Part IV. Both ISO 9001-based and ISO/IEC 27001-based approaches may be used where adapted to meet those requirements. BSI TR-03183-H describes the latter approach (see Section 1.2). The audit team must have competence in the framework used, relevant product technologies and CRA requirements; an existing management-system certificate does not replace Module H assessment and surveillance.

8.3 Competence Requirements for CRA-Module H Notified Bodies

The tables below list the competence requirements for CRA-Module H Notified Bodies, organised by the three requirement categories introduced in Section 3.

Table 17. CRA-Module H: Specific requirements related to the scope of accreditation

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCE
Product-specific conformity assessment capability	Capability to assess the manufacturer's quality-system design and development controls for the product categories or families within scope	EA-2/17 S1 M:2026, Table 1 and Key "pk", referencing EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; Regulation (EU) 2024/2847, Annex I, Part I; Annex VIII, Part IV, points 3.1–3.3; Annexes III and IV, where applicable

Table 18. CRA-Module H: Specific requirements related to the type of conformity assessment activity

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCE
Competence to assess the manufacturer's management processes, to attest its capability to ensure the control of processes, and the consistent meeting of quality objectives	**Evaluation of the manufacturer's quality-system** design, objectives, management responsibilities, planning, support, performance evaluation and improvement. Assessment of the framework used, whether based on ISO 9001, ISO/IEC 27001 or another appropriate approach, against the CRA Module H requirements, including review of relevant examination and test records	ISO/IEC 17021-1:2015, clauses 7.1, 7.2 and Annex A; Reg. (EU) 2024/2847, Annex VIII, Part IV, points 3.2–3.3
Capability to assess development and vulnerability-handling controls within the manufacturer's quality system against the applicable CRA Annex I requirements	**Design and development controls**: assessment of how harmonised standards, common specifications or alternative technical measures are used to demonstrate conformity with Annex I, Part I. Where standards or specifications are not applied, or provide only partial coverage, assess the adequacy of the manufacturer's alternative measures. Review the design and development arrangements and evidence required by Annex VIII, Part IV, considering product risks. An SDLC may support these	EA-2/17 S1 M:2026, Table 1 and Key "pk", referencing EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; Reg. (EU) 2024/2847, Annex I, Parts I and II; Annex VII; Annex VIII, Part IV, points 3.2–3.3 and 4; ISO/IEC 30111:2019; ISO/IEC 29147:2018; ISO/IEC 27006-1:2024, clause 7, where applicable to ISMS audit and certification competence

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCE
	arrangements, but its existence is not a separate assessment criterion. **Vulnerability-handling process effectiveness**: assessment of whether the quality system ensures fulfilment of Annex I, Part II, including process responsibilities, implementation evidence, identified deficiencies and corrective action. Verify continued implementation through Module H surveillance	
Competence to assess the quality system's product-specific design and development controls	**Assessment of the quality system's controls** for cybersecurity risk assessment, design verification and component management, using the supporting technical documentation and records. This includes reviewing how the manufacturer addresses intended purpose and reasonably foreseeable use, verifies the security architecture and maintains component and vulnerability information, including the SBOM	EA-2/17 S1 M:2026, Table 1 and Key "pk", referencing EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; Reg. (EU) 2024/2847, Annex I, Parts I and II; Annex VIII, Part IV, points 3.1–3.3; ENISA Draft Document on Personnel Competences for NoBos; ISO/IEC 27006-1:2024, clause 7, where applicable to ISMS audit and certification competence
Outsourced capabilities	Subcontracting requirements as per the standard	ISO/IEC 17021-1:2015, clause 7.5

Table 19. CRA-Module H: Structural and process requirements

REQUIREMENT CATEGORY	REQUIREMENT	STANDARD REFERENCE
General requirements	Legal and contractual matters (5.1); management of impartiality (5.2); liability and financing (5.3)	ISO/IEC 17021-1:2015, clause 5
Structural requirements	Organisational structure and top management (6.1); operational control (6.2)	ISO/IEC 17021-1:2015, clause 6
Information requirements	Public information (8.1); certification documents (8.2); reference to certification and use of marks (8.3); confidentiality (8.4); information exchange between certification body and clients (8.5)	ISO/IEC 17021-1:2015, clause 8
Process requirements	Pre-certification activities (9.1); audit planning (objectives, scope, criteria, team allocation, audit plan. 9.2); initial certification (Stage 1/Stage 2 audits 9.3); conducting audits (9.4); certification decision (9.5); maintaining certification (surveillance, recertification, special audits 9.6); appeals (9.7); complaints (9.8); client records (9.9)	ISO/IEC 17021-1:2015, clause 9

REQUIREMENT CATEGORY	REQUIREMENT	STANDARD REFERENCE
Management system requirements	**Option A** (standalone CAB management system): management system manual, control of documents, control of records, management review, internal audits, corrective actions. **Option B**: a management system compliant with ISO 9001:2015	ISO/IEC 17021-1:2015, clauses 10.2–10.3; ISO 9001:2015

NOTE: Unlike Module B, Module H's structural and process requirements are drawn entirely from ISO/IEC 17021-1 rather than ISO/IEC 17065. As Section 9.3 shows, these requirements are identical between CRA-Module H and RED-Module H. The gap between the two frameworks is confined to the following rows above: scope of accreditation and conformity assessment activity.

9 RED-Module H: CAB Technical Competences

9.1 Scope of Accreditation

In accordance with EA-2/17 M:2026, Sections 5 – 5.2, the accreditation documentation identifies the reference standard that was applied in full. For RED Module H, Annex A identifies EN ISO/IEC 17021-1 with *qa+cd+pk* obligatory requirements. Supplement 2 provides informative examples of scopes. Consequently, the scope of accreditation should identify the following.

a. **The applicable legislation.** This is Directive 2014/53/EU (the RED Directive) and, within the scope of this analysis, the essential requirements in Article 3(3)(d), (e) and (f), as activated by Commission Delegated Regulation (EU) 2022/30.

b. **The conformity assessment procedure used.** Module H conformity is based on full quality assurance as set out in RED Annex IV.

c. **The radio-equipment categories or families covered**. These are structured according to the applicable essential requirements under Article 1 of Commission Delegated Regulation (EU) 2022/30:

   – **Article 3(3)(d)**, radio equipment capable of communicating over the internet, directly or through other equipment;

   – **Article 3(3)(e),** where the equipment processes personal, traffic or location data:

      • internet-connected radio equipment other than the categories listed below;

      • radio equipment designed or intended exclusively for childcare;

      • radio equipment covered by Directive 2009/48/EC (Toy Safety Directive);

      • radio equipment designed or intended, whether exclusively or not, to be worn on, strapped to, or hung from the human body or clothing;

   – **Article 3(3)(f)**, internet-connected radio equipment enabling the holder or user to transfer money, monetary value or virtual currency.

   The accreditation scope should identify both the product family and the applicable Article 3(3) requirement or requirements, taking account of the exclusions in Article 2 of Delegated Regulation (EU) 2022/30.

d. **The applicable product characteristics or specifications.** These include the relevant RED essential requirements and, where applicable, the corresponding harmonised standards, including the relevant parts of the EN 18031 series and any limitations or restrictions attached to their citation in the Official Journal.

A CAB notified for RED Module H must demonstrate the capability to:

1. **assess and approve the manufacturer's quality system** covering the design, manufacture, final product inspection and the testing of radio equipment within its notified scope;
2. assess whether the design controls of the quality system and supporting technical documentation ensure conformity with the applicable RED essential requirements;
3. **assess production and process assurance**, including the controls for maintaining conformity during manufacture, final inspection and testing, and verify their effective implementation through periodic audits;
4. verify the continuing implementation of the approved quality system through periodic audits.

9.2 Standards for Accreditation for Notification

EA-2/17 M:2026, Annex A, identifies EN **ISO/IEC 17021-1** as the obligatory standard for RED Module H, with *qa+cd+pk* obligatory requirements. The standard is applied in full alongside the applicable legislative and additional competence requirements, subject to the transition described in Section 1.2.

Accordingly, the following should be noted.

- **EN ISO/IEC 17021-1** is the overarching accreditation standard governing competence management, impartiality, management-system auditing, review, certification decisions and surveillance.
- **Product-specific professional competence** must be demonstrated under EN ISO/IEC 17021-1 and the applicable RED or CRA requirements. This includes knowledge of the relevant legislation, essential requirements, technical standards, product technologies, associated risks and state-of-the-art.
- Under EA-2/17 M:2026, Annex A, RED Module H includes the obligatory requirements *pk* and *cd*. The *pk* requirements reference competences in product-related professional judgements in EN **ISO/IEC 17020:2012** clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10. The *cd* requirements reference provisions governing conformity judgements and decisions on certification in EN **ISO/IEC 17065:2012** clauses 4.1.2, 4.1.3, 7.5 and 7.6. EN ISO/IEC 17021-1 remains the accreditation standard applied in full.
- EA-2/17 M:2026, Annex A, Note 4, requires Module H bodies accredited against EN ISO/IEC 17021-1 to comply with the **relevant IAF mandatory documents**, subject to the stated precedence of applicable requirements for with notified bodies.
- **ISO 9001** may provide a relevant quality-management reference, but it is not mandated by EA-2/17 M:2026, RED Annex IV or CRA Annex VIII. The applicable assessment criteria are the relevant Module H legislative requirements, harmonised standards and the manufacturer's documented quality-system arrangements. Other frameworks, including ISO/IEC 27001, may also provide relevant evidence where appropriately mapped to those requirements.

9.3 Competence Requirements for RED-Module H Notified Bodies

The tables below list the competence requirements for RED-Module H Notified Bodies, related to the scope of accreditation, organised by the three requirement categories introduced in Section 3.

Table 20. RED-Module H: Specific requirements related to the scope of accreditation

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCE
Product-specific conformity assessment capability	Capability to assess the manufacturer's quality-system design and development controls for the radio-equipment categories or families within scope	EN 18031-1:2024, EN 18031-2:2024, EN 18031-3:2024; RED Directive 2014/53/EU, Articles 3(3)(d), (e), (f); Annex IV, points 3.1–3.3

Table 21. RED-Module H: Specific requirements related to the type of conformity assessment activity

AREA OF COMPETENCE	REQUIREMENT	STANDARD REFERENCE
Competence to assess the manufacturer's management processes, to attest its capability to ensure the control of processes, and the consistent meeting of quality objectives	Competence to evaluate whether the manufacturer's quality system is effective in planning and maintaining the cybersecurity requirements of RED Art. 3(3)(d), (e), (f) throughout the product lifecycle. Evaluation of QMS planning, support, performance-evaluation, and improvement processes	ISO 17021-1:2015, clauses 7.1, 7.2, Annex A; RED Directive 2014/53/EU, Art. 3(3)(d), (e), (f)
Capability to assess CRA vulnerability-handling processes within the approved quality system	RED has no equivalent to the complete CRA Annex I, Part II vulnerability-handling framework. Both procedures assess the relevant design and development arrangements within the manufacturer's quality system; neither comparison establishes a general SDLC requirement	**Not applicable**
Competence to assess the quality system's product-specific design and development controls	Capability to assess whether the manufacturer's quality-system design controls ensure conformity with the applicable RED essential requirements, including review of supporting risk-assessment documentation, design and architecture information, and verification records.	Directive 2014/53/EU, Annex IV, points 3.1–3.3; EN 18031:2024, clause 6, as applicable
Outsourced capabilities	Subcontracting requirements as per the standard	ISO/IEC 17021-1:2015, clause 7.5

Table 22. RED-Module H: Structural and process requirements (identical to Section 8.3)

REQUIREMENT CATEGORY	REQUIREMENT	STANDARD REFERENCE
General requirements	Legal and contractual matters (5.1); management of impartiality (5.2); liability and financing (5.3)	ISO/IEC 17021-1:2015, clause 5
Structural requirements	Organisational structure and top management (6.1); operational control (6.2)	ISO/IEC 17021-1:2015, clause 6
Information requirements	Public information (8.1); certification documents (8.2); reference to certification and use of marks (8.3); confidentiality (8.4); information exchange between certification body and clients (8.5)	ISO/IEC 17021-1:2015, clause 8
Process requirements	Pre-certification activities (9.1); audit planning (objectives, scope, criteria, team allocation, audit plan. 9.2); initial certification (Stage 1/Stage 2 audits 9.3); conducting audits (9.4); certification decision (9.5); maintaining certification (surveillance, recertification, special audits 9.6); appeals (9.7); complaints (9.8); client records (9.9)	ISO/IEC 17021-1:2015, clause 9

REQUIREMENT CATEGORY	REQUIREMENT	STANDARD REFERENCE
Management system requirements	**Option A** (standalone CAB management system): management system manual, control of documents, control of records, management review, internal audits, corrective actions. **Option B**: a management system compliant with ISO 9001:2015	ISO/IEC 17021-1:2015, clauses 10.2–10.3; ISO 9001:2015

9.4 RED – CRA Module H Gap Analysis and Competence Comparison

The structural requirements concerning CAB competence, impartiality, independence and consistent operation are **substantially aligned** across CRA Module H and RED Module H, reflecting the common NLF model and the management-system certification principles of EN ISO/IEC 17021-1.

However, this document identifies **competence gaps in two areas**.

1. **Assessment of product-design and vulnerability-handling controls within the quality system.** Additional competence concerns the arrangements required by CRA Annex VIII, Part IV, points 3.2–3.3 and 4, supporting conformity with Annex I, Parts I and II. This does not establish a general SDLC requirement. RED Module H has no equivalent to the complete CRA vulnerability-handling framework
2. **Product-specific assessment of quality-system design controls**. This competence is present in both frameworks but they address different substantive requirements, i.e. CRA Annex I, Part I, compared with RED Article 3(3)(d), (e) and (f), supported, where applicable, by the EN 18031 series.

The table below provides a comparative mapping of the competence, accreditation, structural, and process requirements applicable to CABs performing CRA and RED conformity assessment activities, against the corresponding requirements applicable to RED Notified Bodies.

Table 23. RED–CRA Module H CAB Competence and Accreditation Requirements (Gap Comparison)

AREA OF COMPETENCE	CRA REFERENCE	RED REFERENCE
Scope-specific competence		
Capability to assess quality-system design and development controls for the product categories or families within scope	CRA Annex I, Part I; Annex VIII, Part IV, points 3.1–3.3; Annexes III and IV, where applicable	RED Article 3(3)(d), (e), (f); Annex IV, points 3.1–3.3; EN 18031 series, as applicable
Conformity-assessment activity competence		
Competence to assess the manufacturer's management processes, to attest its capability to ensure the control of processes, and the consistent meeting of quality objectives	ISO 17021-1:2015, clauses 7.1, 7.2, Annex A	Identical
Capability to assess development and vulnerability-handling controls within the quality system against the applicable CRA Annex I requirements	EA-2/17 S1 M:2026, Table 1 and Key "pk", referencing EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; Reg. (EU) 2024/2847, Annex I, Parts I and II; Annex VII; Annex	**No equivalent to the complete CRA vulnerability-handling framework; RED quality-system design controls remain applicable**

AREA OF COMPETENCE	CRA REFERENCE	RED REFERENCE
	VIII, Part IV, points 3.2–3.3 and 4; ISO/IEC 30111:2019 and ISO/IEC 29147:2018	
Competence to assess the quality system's product-specific design and development controls	EA-2/17 S1 M:2026, Table 1 and Key "pk"; EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; CRA Annex I, Part I; Annex VII; Annex VIII, Part IV, points 3.1–3.3	EA-2/17 M:2026, Annex A and Key "pk"; EN ISO/IEC 17020:2012 clauses 6.1.2, 6.1.3 and 6.1.6–6.1.10; RED Article 3, as applicable; Annex IV, points 3.1–3.3
Outsourced capabilities	ISO/IEC 17021-1:2015, clause 7.5	ISO/IEC 17021-1:2015, clause 7.5
Structural and process requirements		
General requirements	ISO/IEC 17021-1:2015, clause 5	Identical
Structural requirements	ISO/IEC 17021-1:2015, clause 6	Identical
Information requirements	ISO/IEC 17021-1:2015, clause 8	Identical
Process requirements	ISO/IEC 17021-1:2015, clause 9	Identical
Management system requirements	ISO/IEC 17021-1:2015, clauses 10.2–10.3; ISO 9001:2015	Identical

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

TP-01-26-027-EN-N

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-820-4

Publications Office
of the European Union