TLP - CLEAR

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Technical Competence Requirements

For CRA Notified Bodies

JUNE 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 here: www.enisa.europa.eu.

CONTACT

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

AUTHORS

ENISA

Table of Contents

1. Introduction

1.1 Background

In line with DG.CNCT.H2 request[1], this document is ENISA's contribution on the competence requirements for the notified bodies that will be allowed to perform conformity assessment activities on behalf of the vendors of products with digital elements to demonstrate their compliance to the Cyber Resilience Act (CRA).

The notified bodies (NBs) should be assessed by the Notifying Authorities (NAs) and others bodies involved in the assessment, designation and monitoring of notified bodies. The conformity assessment bodies (CABs) wishing to be notified could use the accreditations against the preferred ISO 17000 series standards[2] in order to demonstrate the conformity with the requirements. In this case, National Accreditation Bodies (NABs) should be involved in the assessment and monitoring.

The Notifying Authorities will remain solely responsible for the all the processes: assessment, monitoring, designation and notification even they may delegate some of these functions to others bodies.

As the requirements for CABs wishing to be notified should be evaluated by the Notifying Authorities, the personnel for Notifying Authorities should have the knowledge, experience and training to assess all requirements for CABs wishing to be notified.

1.2 Scope

The document focuses on high-level competences which will be required to perform conformity assessment activities, in particular the experience and training requirements for the personnel employed by a CAB wishing to be notified (CRA NB) – especially those used as auditors / evaluators. These competences need to be complemented with the specific competences required to demonstrate conformity of products with the harmonised standards that are currently under development[3].

As the document focuses on competence requirements, it does not fully cover conformity to conformity assessment standards (*e.g.*, the application of processes is not covered, except from a competence viewpoint). Nevertheless, it uses the terminology defined for harmonised standard EN ISO/IEC 17000 [1], and it assumes that the activities are organised following the principles of the EN ISO/IEC 17065 [2] or EN ISO/IEC 17021-1 [3] standards.

This document does not cover legal requirements, including proof of liability insurance, organisational requirements, including independence and impartiality, processes requirements, including internal Quality System, facilities requirements, or subcontracting requirements.

[1] May 8, 2025, Ares(2025)6660950
[2] The report from the EA Accreditation for Notification project defined the preferred standard for Module B as EN ISO/IEC 17065, and the preferred standard for Module H as EN ISO/IEC 17021-1.
https://european-accreditation.org/wp-content/uploads/2023/04/AFN-Project-April-2025.pdf
[3] https://www.cencenelec.eu/media/CEN-CENELEC/News/Newsletters/2025/m_606_work_programme_final.pdf

1.3 Relevant conformity assessment standards

In order to produce the following document, the following standards have been used:

- EN ISO/IEC 17065 is the harmonised standard for the certification of products, services and processes, relevant for product-related activities.
- EN ISO/IEC 17021-1 is the harmonised standard for the certification of management systems, relevant in particular for activities related to quality management systems and quality assurance systems.
- EN ISO/IEC 17020 [4] and EN ISO/IEC 17025 [5] are the harmonised standards for respectively, inspection and testing, relevant to some product-related activities.
- EN ISO/IEC 17000 defines common terminology for conformity assessment, here complemented by some terminology related to competences and their assessment defined in EN ISO/IEC 17024, the standard for the certification of persons.
- ISO/IEC TS 17027 [6] defines additional terminology related to competences of persons
- ISO/IEC 19896-3 [7] defines knowledge, skills and effectiveness requirements for Common Criteria evaluators.

2. Basic Concepts

This first part provides a general overview of the personnel competence requirements for the key roles in CABs wishing to be notified.

2.1 Regulation

Article 39 of the CRA defines the requirements relating to notified bodies, and paragraph 7 focuses on the competences of the personnel:

> *7. The personnel responsible for carrying out conformity assessment activities shall have the following:*
> *(a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;*
> *(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;*
> *(c) appropriate knowledge and understanding of the essential cybersecurity requirements set out in Annex I, of the applicable harmonised standards and common specifications, and of the relevant provisions of Union harmonisation legislation and implementing acts;*
> *(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.*

These requirements are a basis, but they need to be interpreted in the light of the competence requirements defined in the 17000 family of standards. The ISO/IEC 17000 series of standards also provides a means of assessing compliance with the generic requirements for all sectors. However, accreditation under the ISO/IEC 17000 series or equivalent is neither required nor necessarily sufficient to justify designation as a notified body under CRA, as the requirements have to be defined by the notifying authority in each Member State.

Nevertheless, the aim of the present document is to define competence requirements that can be used by Notifying Authorities and National Accreditation Bodies across the EU with the objective to harmonise the practices across Member States.

2.2 Roles

The roles are directly inspired from the roles defined in the ISO/IEC 17000 series of standards:

- An **evaluator** is member of the evaluation team, who will perform evaluation tasks.
- A **lead evaluator** is the person who is responsible for the evaluation of a product.
- An **evaluation team** is a team of persons in charge of the evaluation of a product, including one lead evaluator, one or more evaluators, and as required, additional members such as technical experts and observers.

NOTE: The lead evaluator may be the only evaluator in the evaluation team.
NOTE: Technical experts do not need to demonstrate the competences of an evaluator, but they can only perform activities under the supervision of an evaluator.

The personnel preparing an evaluation is in charge for a given product or group of products to review the application, to determine the specific competences required for the evaluation team, to select the evaluation team members, and to determine the evaluation time.

NOTE: This role is usually endorsed by management personnel who interact with clients before the start of the evaluation.

The personnel reviewing reports and making certification decisions are in charge of ensuring that the evaluation has been performed according to the rules defined in the conformity assessment scheme.

NOTE: As per EN ISO/IEC 17065, the personnel reviewing reports must be independent from the evaluation team.

2.3 Competences, knowledge and skills

A competence is defined as the “ability to apply knowledge and skills to achieve intended results” in EN ISO/IEC 17021-1 (3.7). It is clearly composed of two aspects:

- knowledge and skills;
- the ability to apply them to achieve intended results.

Competence requirements therefore need to cover both aspects as well. ISO/IEC TS 17027 adds more relevant definitions:

- An ability is defined as the capacity to perform an activity (2.1).
- Knowledge is defined as facts, information, truths, principles or understanding acquired through education, training, experience or other means (2.56, slightly modified to match 2.74).
- A skill is defined as ability to perform a task or activity with a specific intended outcome acquired through education, training, experience or other means (2.74).

3. Required Knowledge and Skills

3.1 Overview

The table below, inspired from CEN TS 18072's Annex A [8], defines the knowledge and skills required for the different roles, which are then defined in greater details in the rest of the section.

In the table below, a "B" indicates a competence requirement for Module B assessments, an "H" indicates a competence requirement for Module H assessments and an "(X)" indicates a conditional competence requirement (typically, a requirement for all stakeholders involved in a related activity). The assumption is here that a conformity assessment body may be notified for performing only some activities (e.g., Module B assessments, but no module H assessments). A "X*" indicates a partial coverage of a competence requirement.

The following guidelines can be used:

- A mark in the "**Evaluator**" column indicates knowledge and skills that are required for all relevant evaluators.
- A mark in the "**Evaluation lead**" column indicates knowledge and skills that are required for lead evaluators, in addition to the other skills of an evaluator, or with higher expectation levels.
- A mark in the "**Evaluation team**" column indicates knowledge and skills that are required for at least one member of the evaluation team.
- A mark in the "**Personnel preparing the evaluation**" column indicates knowledge and skills that are required for the persons involved in the application review to determine the evaluation team competence required, to select the evaluation team members and to determine the evaluation time
- A mark in the "**Personnel reviewing reports and making decisions**" column indicates knowledge and skills that are required for the person in charge of reviewing reports and making conformity assessment decisions.

In all cases, additional details are provided below.

Figure 2: *Summary of knowledge and skills*

Competences	Evaluator	Evaluation lead	Evaluation team	Personnel preparing the evaluation	Personnel reviewing reports and making decisions
Knowledge of common industry practices	See 3.2.1	See 3.2.1	See 3.2.1	See 3.3.1	See 3.4.1
principles of cybersecurity	B/H			B/H	B/H
design and development of products with digital elements	B/H				B/H

Competences	Evaluator	Evaluation lead	Evaluation team	Personnel preparing the evaluation	Personnel reviewing reports and making decisions
quality assurance systems for the development and production of products with digital elements	H				H
technical knowledge of products with digital elements			B/H		
Knowledge of information security terminology, principles, practices and techniques	See 3.2.2	–	See 3.2.2	See 3.3.2	See 3.4.2
cybersecurity specific terminology and documentation structures, hierarchy and interrelationships	B/H			B/H	B/H
cybersecurity aspects of the design and development of products with digital elements, including secure development life cycle	(B/H)		B/H		B/H
cybersecurity management related tools, methods, techniques and their application to the design, development and production of products with digital elements	(B/H)		B/H		(B)/H
common vulnerabilities, vulnerability identification and vulnerability management	B/H			B/H	B/H
cybersecurity risk assessment and risk management	B/H				B/H
cryptographic mechanisms	B		H		B/(H)
current technology where information security may be relevant or an issue			B/H		
legal and regulatory requirements relevant to cybersecurity			B/H		B/H
Knowledge of conformity assessment terminology, principles, practices and techniques	See 3.2.3	–	See 3.2.3	See 3.3.3	See 3.4.3
conformity assessment specific terminology and documentation structures, hierarchy and interrelationships	B/H			B/H	B/H
evaluation processes and procedures	(B/H)	B/H	B/H		B/H
evaluation principles, practices and techniques	(B/H)	B/H	B/H		B/H
Evaluation skills	See 3.2.4	See 3.2.4	See 3.2.4	–	–
testing skills	(B)		B/H		
examination skills	(B/H)		B/H		

Competences	Evaluator	Evaluation lead	Evaluation team	Personnel preparing the evaluation	Personnel reviewing reports and making decisions
auditing skills	H		B/H		
language skills	B/H				
note-taking and report-writing skills	B/H	B/H			
presentation skills	H	B/H			
interviewing skills	H		B		
Knowledge of specific standards and normative documents	See 3.2.5	–	See 3.2.5	See 3.3.4	See 3.4.4
relevant conformity assessment schemes, information security standards and other normative documents used in the conformity assessment process	B/H			B/H	B/H
relevant cybersecurity requirements, as defined in schemes, standards and other normative documents			B/H		
relevant cybersecurity evaluation methodologies, as defined in schemes, standards and other normative documents			B/H		
Knowledge of conformity assessment body's processes	See 3.2.6	–	–	See 3.3.5	See 3.4.5
CAB general policies and processes, including information security policies and processes	B/H			B/H	B/H
CAB processes and procedures for the evaluation of products with digital elements	B				B
CAB processes and procedures for the audit of quality management systems	H				H
CAB approved evaluation methods	(B/H)				
requirements of the conformity assessment schemes for which the CAB is authorised to work	(B/H)			(B/H)	(B/H)
Knowledge of client's business sector	See 3.2.7	–	See 3.2.7	See 3.3.6	See 3.4.6
the legal and regulatory requirements in the particular information security field, geography and jurisdictions(s)			B/H		
information security risks related to the client's business sector	B/H				

Competences	Evaluator	Evaluation lead	Evaluation team	Personnel preparing the evaluation	Personnel reviewing reports and making decisions
generic terminology, processes and technologies related to the client's business sector	B/H			B/H	B/H
relevant business sector practices	(B/H)				
Knowledge of client products, processes and organisation	–	–	See 3.2.8	See 3.3.7	See 3.4.7
the impact of organization type, size, governance, structure, functions and relationships on the design, development and production of the product with digital elements			B/H	B/H	
categories of products with digital services developed by the client			B/H		B/H
Evaluation management skills	See 3.2.9	See 3.2.9	–	–	–
conducting and managing evaluation activities	B/H	B/H			
knowledge and skills to manage the evaluation process and the evaluation team		B/H			

3.2 Competences for performing evaluations

This section covers the competences of the personnel performing evaluations, which includes the individual evaluators, the evaluation lead, and the evaluation team.

> **NOTE**: Evaluation covers all selection and determination activities, including inspection, audit, testing, validation and verification.

3.2.1 Knowledge of common industry practices

Every evaluator involved in the evaluation of products with digital elements shall have knowledge of:

- principles of cybersecurity;
- design and development of products with digital elements.

This is general knowledge, which shall be understood by all personnel involved in the evaluation, even if their tasks are very specialised.

In addition, evaluators participating to assessments based on Module H shall have knowledge of quality assurance systems for the development and production of products with digital elements.

Finally, collectively, the evaluation team involved in the evaluation of products with digital elements shall have technical knowledge of products with digital elements. This is much more

specific knowledge, so each member of the team is expected to cover a part of the required knowledge.

3.2.2 Knowledge of information security terminology, principles, practices and techniques

Every evaluator involved in the evaluation of products with digital elements shall have knowledge of:

- cybersecurity specific terminology and documentation structures, hierarchy and interrelationships;
- as applicable, cybersecurity aspects of the design and development of products with digital elements, including secure development life cycle;
- as applicable, cybersecurity management related tools, methods, techniques and their application to the design, development and production of products with digital elements;
- common vulnerabilities, vulnerability identification and vulnerability management;
- cybersecurity risk assessment and risk management;
- as applicable, cryptographic mechanisms.

NOTE: When a topic is marked as “as applicable”, then it only applies to the evaluators who need the knowledge in order to perform their evaluation activities. For instance, a tester may not need knowledge on design and development, but an inspector or an auditor may need that knowledge, and may also need some knowledge on cybersecurity management related tools and techniques.

In addition, regardless of the type of evaluation, the evaluation team involved in the evaluation of products with digital elements shall have technical knowledge of all these, as well as of

- current technology where information security may be relevant or an issue;
- legal and regulatory requirements relevant to cybersecurity.

NOTE: The use of the adjective “current” indicates that it is particularly important for this matter to keep the knowledge on technologies up-to-date.

NOTE: Contrarily to CEN TS 18072, which only requires knowledge about legal and regulatory requirements for certifiers, we have considered that these requirements needed to be covered in the evaluation team in the context of CRA.

3.2.3 Knowledge of conformity assessment terminology, principles, practices and techniques

Every evaluator involved in the evaluation of products with digital elements shall have knowledge of:

- conformity assessment specific terminology and documentation structures, hierarchy and interrelationships;
- as applicable, evaluation processes and procedures;
- evaluation principles, and as applicable, evaluation practices and techniques.

In addition, evaluation leads shall have knowledge of:

- evaluation processes and procedures;
- evaluation principles, practices and techniques.

NOTE: This element is more detailed than in CEN TS 18072, and its content could be discussed. In particular, we propose to only require evaluators to know the processes and procedures, as well as the practices and techniques that are relative to the evaluation activities that they perform. Evaluation leads, on the other hands, need to have transversal knowledge of these aspects.

3.2.4 Evaluation skills

Every evaluator involved in the evaluation of products with digital elements shall have technical skills, including as applicable:

- testing skills;
- inspection skills;
- auditing skills

Inspection skills shall be complemented as required by sufficient competences to form a professional judgment. In addition, every evaluator involved in the evaluation of products with digital elements shall have general skills, including:

- language skills;
- note-taking and report-writing skills;
- as applicable, presentation skills;
- as applicable, interviewing skills.

In addition, collectively, the evaluation team involved in the evaluation of products with digital elements shall have knowledge of testing and inspection skills.

NOTE: For Module H, at least one member of the evaluation team needs to have product-specific competencies, including an assessment of the deliverables provided by the manufacturer [9].

NOTE: For Module B, 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 [9].

Evaluation leads shall have a higher level of report-writing and presentation skills, in order to report the findings to the clients in written and oral forms.

NOTE: The description of the skills needs to be much more detailed, in particular for the technical skills related to product assessment (inspection and testing). This information is likely to be defined in (or easily derived from) harmonised standards. In the meantime, the competences will be linked to the evaluation methodology defined by the CAB to perform the evaluation.

3.2.5 Knowledge of specific standards and normative documents

Every evaluator involved in the evaluation of products with digital elements shall have knowledge of:

- relevant conformity assessment schemes, information security standards and other normative documents used in the conformity assessment process;

NOTE: This is general knowledge, required for all evaluators, and the more specific knowledge of the requirements and methodologies are only required for the evaluation team.

In addition, collectively, the evaluation team involved in the evaluation of products with digital elements shall have knowledge of

- relevant cybersecurity requirements, as defined in schemes, standards and other normative documents;
- relevant cybersecurity evaluation methodologies, as defined in schemes, standards and other normative documents

NOTE: Harmonised standards are expected to provide a reference framework, from which more detailed requirements and activities will be derived. Before the availability of these harmonised standards, ENISA and the JRC have identified a set of standards that may be of interest [10].

3.2.6 Knowledge of conformity assessment body's processes

Every evaluator involved in the evaluation of products with digital elements shall have knowledge of:

- CAB general policies and processes, including information security policies and processes;
- for evaluators involved in Module B assessments, CAB processes and procedures for the evaluation of products with digital elements;
- for evaluators involved in Module H assessments, CAB processes and procedures for the audit of quality assurance systems;
- as applicable, CAB approved evaluation methods;
- as applicable, requirements of the conformity assessment schemes for which the CAB is authorised to work.

NOTE: More details may be required about the processes that are relevant for a given type of conformity assessment, but evaluators may be specialised in a particular kind of assessment. For instance, when implementing Module B, testing procedures have to be known, whereas for Module H, the focus would be on auditing procedures, which is why "as applicable" has been used here.

3.2.7 Knowledge of client's business sector

Every evaluator involved in the evaluation of products with digital elements shall have knowledge of:

- information security risks related to business sector;

- generic terminology, processes and technologies related to the client's business sector;
- as applicable, relevant business sector practices.

In addition, collectively, the evaluation team involved in the evaluation of products with digital elements shall have knowledge of the legal and regulatory requirements in the particular information security field, geography and jurisdictions(s).

NOTE: There needs to be a discussion about the relationship between "business sectors" and the "product categories" defined in the CRA. Harmonised standards will define risks, and they are likely to identify specific technical aspects and business practices specific to a business sector. A single business sector may correspond to several product categories (*e.g.*, the semiconductor sector covers several product categories), so a good practice would be to list the CRA product categories covered by the business sector.

3.2.8 Knowledge of client products, processes and organisation

Collectively, the evaluation team involved in the evaluation of products with digital elements shall have knowledge of:

- the impact of organization type, size, governance, structure, functions and relationships on the design, development and production of the product with digital elements;
- the categories of products with digital services developed by the client.

The CRA requires in Annex VIII, Part IV, section 3.3 that the "team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and shall have knowledge of the applicable requirements set out in this Regulation". Knowledge related to the product corresponds to the ability to make professional judgments related to the product requirements, which should be demonstrated via application of EN ISO/IEC 17020 clauses 6.1.2 to 6.1.3, and 6.1.6 to 6.1.10 [11].

3.2.9 Evaluation management skills

Every evaluator involved in the evaluation of products with digital elements shall be skilled at conducting and managing evaluation activities.

In addition, every evaluation lead shall have deeper knowledge of the evaluation activities, as well as the knowledge and skills to manage the certification evaluation process and the evaluation team.

NOTE: Every evaluator shall have the ability to manage its own activities and report to the evaluation lead, who shall then have the required skills to support the evaluators and to coordinate the evaluators in the team.

3.3 Competences for preparing evaluations

This section covers the competences of the personnel involved in the application review to determine the evaluation team competence required, to select the evaluation team members and to determine the evaluation time.

NOTE: These personnel may be involved in the performance of evaluations or not, but they need to have enough knowledge to understand how an evaluation is performed, the set of skills that will

be required for a given evaluation and the time required to perform the evaluation However, this role does not require any operational skills on the performance of evaluation activities.

3.3.1 Knowledge of common industry practices

Personnel involved in the application review and evaluation preparation shall have knowledge of principles of cybersecurity.

3.3.2 Knowledge of information security terminology, principles, practices and techniques

Personnel involved in the application review and evaluation preparation shall have knowledge of

- cybersecurity specific terminology and documentation structures, hierarchy and interrelationships;
- vulnerability management processes.

3.3.3 Knowledge of conformity assessment terminology, principles, practices and techniques

Personnel involved in the application review and evaluation preparation shall have knowledge of: conformity assessment specific terminology and documentation structures, hierarchy and interrelationships.

3.3.4 Knowledge of specific standards and normative documents

Personnel involved in the application review and evaluation preparation shall have knowledge of relevant conformity assessment schemes, information security standards and other normative documents used in the conformity assessment process.

3.3.5 Knowledge of conformity assessment body's processes

Personnel involved in the application review and evaluation preparation shall have knowledge of

- conformity assessment body general policies and processes, including information security policies and processes;
- as applicable, requirements of the conformity assessment schemes for which the CAB is authorised to work.

3.3.6 Knowledge of client's business sector

Personnel involved in the application review and evaluation preparation shall have knowledge of generic terminology, processes and technologies related to the client's business sector.

3.3.7 Knowledge of client products, processes and organisation

Personnel involved in the application review and evaluation preparation shall have knowledge of the impact of organization type, size, governance, structure, functions and relationships on the design, development and production of the product with digital elements.

3.4 Competences for reviewing reports and making decisions

This section covers the competences of the personnel in charge of reviewing reports and making conformity assessment decisions.

> **NOTE**: These personnel are essential in a conformity assessment body. They also need to be independent from those performing the conformity assessment activities, while mastering many of their competences, with the notable exception of the skills to actually perform the conformity assessment activities. These personnel provide the guarantee that the processes and procedures defined by the notified body are appropriately applied in every conformity assessment project.

3.4.1 Knowledge of common industry practices

Personnel in charge of reviewing reports and making conformity assessment decisions shall have knowledge of:

- principles of cybersecurity;
- design and development of products with digital elements;
- for reviews and decisions related to Module H conformity assessments, quality management systems for the development and production of products with digital elements.

3.4.2 Knowledge of information security terminology, principles, practices and techniques

Personnel in charge of reviewing reports and making conformity assessment decisions shall have knowledge of:

- cybersecurity specific terminology and documentation structures, hierarchy and interrelationships;
- as applicable, cybersecurity aspects of the design and development of products with digital elements;
- as applicable and at least for reviews and decisions related to Module H conformity assessments, cybersecurity management related tools, methods, techniques and their application to the design, development and production of products with digital elements;
- common vulnerabilities, vulnerability identification and vulnerability management;
- cybersecurity risk assessment and risk management;
- as applicable and at least for reviews and decisions related to Module B conformity assessments, cryptographic mechanisms
- legal and regulatory requirements relevant to cybersecurity.

3.4.3 Knowledge of conformity assessment terminology, principles, practices and techniques

Personnel in charge of reviewing reports and making conformity assessment decisions shall have knowledge of:

- conformity assessment specific terminology and documentation structures, hierarchy and interrelationships;
- evaluation processes and procedures;

- evaluation principles, practices and techniques.

3.4.4 Knowledge of specific standards and normative documents

Personnel in charge of reviewing reports and making conformity assessment decisions shall have knowledge of relevant conformity assessment schemes, information security standards and other normative documents used in the conformity assessment process.

3.4.5 Knowledge of conformity assessment body's processes

Personnel in charge of reviewing reports and making conformity assessment decisions shall have knowledge of:

- CAB general policies and processes, including information security policies and processes;
- for reviews and decisions related to Module B conformity assessments, CAB processes and procedures for the evaluation of products with digital elements;
- for reviews and decisions related to Module H conformity assessments, CAB processes and procedures for the audit of quality assurance systems;
- if applicable, requirements of the conformity assessment schemes for which the CAB is authorised to work.

NOTE: This knowledge is essential for reviewers, which focuses on the appropriate application of the CAB's processes and procedures.

3.4.6 Knowledge of client's business sector

Personnel in charge of reviewing reports and making conformity assessment decisions shall have knowledge of generic terminology, processes and technologies related to the client's business sector.

3.4.7 Knowledge of client's products, processes and organisations

Personnel in charge of reviewing reports and making conformity assessment decisions shall have knowledge of the categories of products with digital services developed by the client.

NOTE: In the context of CRA, this knowledge is important for reviewers, because of the specific practices that may apply to different categories of products.

4. Competence requirements

Competence requirements complement the knowledge and skills requirements by requirements on the education, experience, training and other aspects required for every role.

4.1 Parameters

As indicated in the introduction, a competence is an ability to apply knowledge and skills. A notified body shall assess the competence of the employees performing conformity assessment tasks, using available tools, including:

- Requiring educational credentials (diplomas) on a given field and level.
- Requiring practical experience in a given role and field.
- Administering trainings to personnel.
- Requiring a specific personal certification.

Because the cybersecurity area remains relatively recent, and because there are very limited opportunities to acquire conformity assessment skills through education, it is important to remain very careful with educational requirements (*i.e.*, requiring a degree in cybersecurity). Many practitioners are likely to have a general computer science degree, complemented by experience and practical trainings in cybersecurity. It is therefore recommended to define several equivalent profiles for a given qualification level.

For instance, the requirements for an auditor in a Module H assessment could be as follows:

- A Master degree in cybersecurity, plus two years of auditing practice as a junior auditor.
- A Master degree in a field related to cybersecurity[4], plus four years of practice, including at least two years of auditing practice as a junior auditor.
- A Bachelor degree in cybersecurity, plus four years of practice, including at least two years of auditing practice as a junior auditor.
- A Bachelor degree in a field related to cybersecurity, plus six years of practice, including at least two years of auditing practice as a junior auditor.

Of course, the combinations depend on the role, but it is important to be flexible enough, in order to allow different career paths. In addition, these requirements should be adapted to local practices, and could be open to alternative paths, such as continuing education and other training opportunities.

On a different profile, the requirements for a penetration tester could be quite different (only one example provided, but variants should be considered in a way similar to those proposed for auditors above):

[4] This needs to be further refined, but it would typically include degrees in computer science and where relevant, in electronics, as well as some management degrees for some aspects of Module H.

- A Master degree in computer science or electronics, evidence of training related to the use of specific equipment, plus on-the-job training in for at least one year on at least three relevant evaluations;

  NOTE: This needs to be further discussed, but for the initial version of this document, and since the main reason for appointing notified bodies is to have them involved in the definition and implementation of initial rules, it seems interesting to focus on practical experience, both for the personnel and for the entity, requiring significant experience in the assessment of the cybersecurity of products with digital elements. In addition, education requirements could be replaced by personal certifications, and the definition of junior auditor need to be refined.

In addition, as indicated in Annex of CRA, in the case of Module H, at least one of the members of the auditing team needs to have experience "as an assessor in the relevant product field and product technology".

NOTE: This requirement needs to be considered carefully, since it is quite strong, possibly stronger than for a product evaluator (since many of the competences are assigned to the evaluation team rather than an individual evaluator). It may be interesting to define a specific category for this specific role.

4.2 Input from EA's Accreditation for Notification (AfN) Project

Europe Accreditation (EA) has issued document EA:2/17 [11] about accreditation for notification purposes, and they are regularly publishing updates for this project. Their 2025 update [9] mentions CRA, and the preferred standards that are proposed are:

- for Module B, "EN ISO/IEC 17065 + testing and inspection capability will be required"; and
- for Module H, "EN ISO/IEC 17021-1 + auditor competence must include specific product knowledge".

In addition, EA 2/17 provides additional details in Annex B. For Module B:

- for testing, "fulfilment of the applicable requirements of clause 6 and 7 (except 7.9) in EN ISO/IEC 17025:2017 shall be demonstrated"; and
- for product knowledge, the requirement is the ability to make professional judgments related to product requirements, so "fulfilment of clauses 6.1.2, 6.1.3 and 6.1.6 to 6.1.10 of EN ISO/IEC 17020:2012 shall be demonstrated".

And for Module H, only product knowledge applies, so the requirement is the ability to make professional judgments related to product requirements, so "fulfilment of clauses 6.1.2, 6.1.3 and 6.1.6 to 6.1.10 of EN ISO/IEC 17020:2012 shall be demonstrated".

4.3 Management of competences

The present document only covers the competence requirements, but it is important to keep in mind that the actual requirement from EN ISO/IEC 17065 (in section 6.1.2) is about the "management of competence for personnel involved in the certification process".

It is important to keep in mind that the availability of competent personnel is not only to be assessed at a point in time before accreditation or notification, but also that a process is in place to manage these

competences over time. The operating effectiveness of this process also needs to be checked when the accreditation or notification is reviewed or renewed by a NA or NAB.

5. References

[1] ISO/IEC, *ISO/IEC 17000:2020(en) Conformity assessment — Vocabulary and general principles,* 2020.

[2] ISO/IEC, *ISO/IEC 17065:2012(en) Conformity assessment — Requirements for bodies certifying products, processes and services,* 2012.

[3] ISO/IEC, *ISO/IEC 17021-1:2015(en) Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements,* 2015.

[4] ISO/IEC, *ISO/IEC 17020:2026(en) Conformity assessment — Requirements for bodies performing inspection,* 2026.

[5] ISO/IEC, *ISO/IEC 17025:2017(en) General requirements for the competence of testing and calibration laboratories,* 2017.

[6] ISO/IEC, "ISO/IEC TS 17027:2014(en) Conformity assessment — Vocabulary related to competence of persons used for certification of persons," 2014.

[7] ISO/IEC, "ISO/IEC 19896-3:2025(en) Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 3: Knowledge and skills requirements for evaluators and reviewers according t," 2025.

[8] CN/CENELEC, "CEN/CLC/TS 18072:2025 Requirements for Conformity Assessment Bodies certifying Cloud Services," 2025.

[9] European Accreditation, "EA Accreditation for Notification (AfN) Project Report - Updated April 2025," 2025. [Online]. Available: https://european-accreditation.org/wp-content/uploads/2025/10/AFN-Project-April-2025.pdf. [Accessed 22 April 2026].

[10] JRC & ENISA, "Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis," 2024. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping. [Accessed 22 April 2026].

[11] European Accreditation, "EA-2/17:2020 EA Document on Accreditation for Notification Purposes," 2020. [Online]. Available: https://european-accreditation.org/wp-content/uploads/2018/10/ea-2-17-m.pdf. [Accessed 22 April 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 here: www.enisa.europa.eu.

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

Publications Office
of the European Union