



BSI Standards Publication

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 to the ISO/IEC 15408 series and ISO/IEC 18045

National foreword

This British Standard is the UK implementation of EN ISO/IEC 19896-3:2025. It is identical to ISO/IEC 19896-3:2025. It supersedes BS EN ISO/IEC 19896-3:2023, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/3, Security Evaluation, Testing and Specification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 25866 0

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English version

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 to the ISO/IEC 15408 series and
ISO/IEC 18045 (ISO/IEC 19896-3:2025)

Sécurité de l'information, cybersécurité et protection
de la vie privée - Exigences relatives aux compétences
du personnel des organismes d'évaluation de la
conformité de la sécurité TI - Partie 3: Exigences en
matière de connaissances et de compétences pour les
évaluateurs et les examinateurs conformément à la
série ISO/IEC 15408 et à l'ISO/IEC 18045 (ISO/IEC
19896-3:2025)

Informationssicherheit, Cybersicherheit und Schutz
der Privatsphäre - Anforderungen an die Kompetenz
des Personals von Konformitätsbewertungsstellen für
IT-Sicherheit - Teil 3: Anforderungen an die
Kenntnisse und Fähigkeiten von Evaluatoren und
Zertifizierern nach ISO/IEC 15408 und ISO/IEC 18045
(ISO/IEC 19896-3:2025)

This European Standard was approved by CEN on 25 November 2025.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO/IEC 19896-3:2025) has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" in collaboration with Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2026, and conflicting national standards shall be withdrawn at the latest by May 2026.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 19896-3:2023.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 19896-3:2025 has been approved by CEN-CENELEC as EN ISO/IEC 19896-3:2025 without any modification.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	2
3.1 Terms and definitions	2
3.2 Abbreviated terms	2
4 Knowledge	2
4.1 Knowledge required for evaluators	2
4.1.1 General	2
4.1.2 Knowledge of the ISO/IEC 15408 series and ISO/IEC 18045	3
4.1.3 Knowledge of the assurance paradigm	5
4.1.4 Knowledge of information security	6
4.1.5 Knowledge of the technology	7
4.2 Knowledge required for reviewers	8
4.2.1 General	8
4.2.2 Knowledge of the ISO/IEC 15408 series and ISO/IEC 18045	9
4.2.3 Knowledge of the assurance paradigm	10
4.2.4 Knowledge of information security	12
4.2.5 Knowledge of technology	13
5 Skills	14
5.1 Skills required for evaluators	14
5.1.1 General	14
5.1.2 Basic evaluation skills	14
5.1.3 Core evaluation skills regarding ISO/IEC 15408-3 and ISO/IEC 18045	15
5.1.4 Skills required for specific security assurance classes	16
5.1.5 Skills required for specific security functional requirement classes	17
5.1.6 Skills required for specific technology	17
5.2 Skill required for reviewers	17
5.2.1 Basic review skills	17
5.2.2 Core review skills regarding ISO/IEC 15408-3 and ISO/IEC 18045	18
5.2.3 Skills required for specific security assurance classes	18
5.2.4 Skills required for specific security functional requirement classes	19
5.2.5 Skills required for specific technology	19
Annex A (informative) Technology types: knowledge and skills	20
Annex B (informative) Examples of knowledge and skills required for evaluating security assurance requirement classes	27
Annex C (informative) Examples of knowledge required for evaluating security functional requirement classes	40
Bibliography	44

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 19896-2:2018), which has been technically revised.

The main changes are as follows:

- completely reworked the requirements for evaluators, including restructuring of the content;
- added requirements for personnel reviewing IT security conformance assessment activities.

A list of all parts in the ISO/IEC 19896 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functionality of information technology (IT) products and for assurance measures applied to these IT products during a security evaluation. Many review and evaluation schemes as well as review bodies have been developed using the ISO/IEC 15408 series and ISO/IEC 18045 as a basis, which permits comparability between the results of evaluation projects.

The evaluation process usually relies on both pre-defined tests/methods for a type of TOE, and TOE-specific tests/methods that are defined for a given implementation of the TOE. Hence, the competence of the individual evaluators, who are expected not only to apply pre-defined tests/methods but to define and run TOE-specific tests/methods, is key to ensuring the comparability and repeatability of evaluation results which is the foundation for mutual recognition.

This document establishes a baseline for the minimum competence of ISO/IEC 15408 series evaluators and reviewers to ensure harmonized requirements for training ISO/IEC 15408 evaluators and reviewers. It provides specialized requirements for individuals performing IT product security evaluations and reviews to demonstrate their competence according to the ISO/IEC 15408 series and ISO/IEC 18045. ISO/IEC 15408-1 describes the general framework for competences including the various elements thereof: knowledge, skills, experience and education. This document covers knowledge and skills, especially in the following areas.

- Information security
 - Knowledge: information security principles, information security properties, information security threats and vulnerabilities.
 - Skills: understanding information security requirements, the context and the scope of evaluation.
- Information security evaluation
 - Knowledge: knowledge of the ISO/IEC 15408 series and ISO/IEC 18045, laboratory management system.
 - Skills: Basic evaluation skills, core evaluation skills, skills required when evaluating specific security assurance classes, skills required when evaluating specific security functional requirements classes.
- Information systems architecture
 - Knowledge: technology being evaluated.
 - Skills: understanding the interaction of security components and information.
- Information security testing
 - Knowledge: information security testing techniques, information security testing tools, product development lifecycle, test types.
 - Skills: creating and managing an information security test plan, designing information security tests, preparing and conducting information security tests.

The audience for this document includes testing laboratory accreditation bodies, organizations implementing evaluation schemes, laboratories, evaluators and organizations offering professional credentialing.

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 to the ISO/IEC 15408 series and ISO/IEC 18045

1 Scope

This document provides the specialized requirements for individuals to demonstrate competence in performing IT product security evaluations and reviews according to the ISO/IEC 15408 series and ISO/IEC 18045.

NOTE It is possible that evaluators and testers belong to bodies operating under ISO/IEC 17025 and reviewers belong to bodies operating under ISO/IEC 17065.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19896-1, *Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 1: Introduction and concepts*

ISO/IEC 15408-1:—¹⁾, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:—²⁾, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:—³⁾, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

ISO/IEC 18045:—⁴⁾, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

1) Under preparation. Stage at the time of publication: ISO/IEC FDIS 15408-1:2025.

2) Under preparation. Stage at the time of publication: ISO/IEC DIS 15408-2:2025.

3) Under preparation. Stage at the time of publication: ISO/IEC DIS 15408-3:2025.

4) Under preparation. Stage at the time of publication: ISO/IEC FDIS 18045:2025.

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 19896-1, ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 Terms and definitions

3.1.1

supporting document

document that specifies the use of the Common Criteria (CC) or common methodology for information technology security evaluation (CEM) in a particular field or domain of technology

Note 1 to entry: Such a document can be either required or recommended, and generally specifies harmonized interpretations of the CC and CEM where deemed necessary and/or useful.

3.1.2

technical domain

family of information technology (IT) products that require specific technical competencies, especially with regard to the vulnerability analysis, requiring a common understanding of the attack potential for performing the evaluation

3.2 Abbreviated terms

CC	Common Criteria
CEM	common evaluation methodology
cPP	collaborative protection profile
ETR	evaluation technical report
IC	integrated circuit
IT	information technology
PP	protection profile
ST	security target
TSF	TOE security functionality
TSFI	TOE security functionality interface
TOE	target of evaluation

4 Knowledge

4.1 Knowledge required for evaluators

4.1.1 General

[4.1.2](#) to [4.1.5](#) address the knowledge that is required to evaluate according to the ISO/IEC 15408 series and ISO/IEC 18045.

Some knowledge is required for every evaluator independent of their specific task, while other knowledge is required only depending on the specific evaluation task and the TOE to which the evaluator is assigned.

NOTE Previous experience in tasks related to the use of the ISO/IEC 15408 series and its related documents including, but not limited to, performing related work such as review, consultancy, product development, research and specification of requirements, can contribute to the elements of knowledge that are required for competence.

4.1.2 Knowledge of the ISO/IEC 15408 series and ISO/IEC 18045

4.1.2.1 Generic knowledge of the ISO/IEC 15408 series and ISO/IEC 15408 18045

Every evaluator's knowledge shall include:

- a) the terms and definitions defined in ISO/IEC 15408-1:—⁵⁾, Clause 3; ISO/IEC 15408-2:—⁶⁾, Clause 3; and ISO/IEC 15408-3:—⁷⁾, Clause 3;
- b) the terms and definitions defined in ISO/IEC 18045:—⁸⁾ Clause 3; and
- c) the context for evaluations according to the ISO/IEC 15408 series.

4.1.2.2 Knowledge of ISO/IEC 15408-1

Every evaluator shall be able to demonstrate knowledge about the topics required to fulfil their role according to their competence level and on which the person is authorized to work.

Every evaluator's knowledge shall include:

- a) the general model for the ISO/IEC 15408 series given in ISO/IEC 15408-1.

When the evaluator's role and competency level demand it, their knowledge shall include the following relevant items:

- b) tailoring security requirements: operations, dependencies between components and extended components;
- c) specification of protection profiles, modules, configurations and packages;
- d) handling of evaluation results;
- e) specification of security targets;
- f) composition models;
- g) multi-assurance approach; and
- h) modularization concepts.

4.1.2.3 Knowledge of ISO/IEC 15408-2

Every evaluator shall be able to demonstrate knowledge about the security functional requirements (SFRs) of ISO/IEC 15408-2 required to fulfil their role according to their competence level and the technology types on which the evaluator is authorized to work, as well as any dependent SFRs. Examples of the knowledge required by ISO/IEC 15408-2 are given in [Annex C](#).

If the evaluator is required to demonstrate competence in ISO/IEC 15408-2, then knowledge of the respective security functional requirements shall be demonstrated.

5) Under preparation. Stage at the time of publication: ISO/IEC FDIS 15408-1:2025.

6) Under preparation. Stage at the time of publication: ISO/IEC DIS 15408-2:2025.

7) Under preparation. Stage at the time of publication: ISO/IEC DIS 15408-3:2025.

8) Under preparation. Stage at the time of publication: ISO/IEC FDIS 18045:2025.

4.1.2.4 Knowledge of ISO/IEC 15408-3

Every evaluator shall be able to demonstrate knowledge about the security assurance requirements (SARs) given in ISO/IEC 15408-3 required to fulfil their role according to their competence level and that are specified by Security Targets (ST) on which the evaluator is authorized to work. The knowledge of particular SAR components shall include those on which the evaluator is authorized to work. Examples of the knowledge required by ISO/IEC 15408-3 are given in [Annex B](#).

If the evaluator is required to demonstrate competence in ISO/IEC 15408-3, then knowledge of the respective security assurance requirements shall be demonstrated.

4.1.2.5 Knowledge of ISO/IEC 15408-4

If the evaluator is required to demonstrate competence in ISO/IEC 15408-4, then the following shall be demonstrated:

- a) the framework used for deriving evaluation activities from work units in ISO/IEC 18045;
- b) the general model of evaluation methods and evaluation activities; and
- c) defining evaluation activities for extended SARs.

4.1.2.6 Knowledge of ISO/IEC 15408-5

If the evaluator is required to demonstrate competence in ISO/IEC 15408-5, then knowledge about the packages specified in ISO/IEC 15408-5 shall be demonstrated.

4.1.2.7 Knowledge of ISO/IEC 18045

Every evaluator shall demonstrate:

- a) the evaluation process, as described in ISO/IEC 18045:—, Clause 8; and
- b) security evaluation method and activities given in ISO/IEC 18045.

Additionally, every evaluator shall have the necessary knowledge required by the evaluation methods and activities specified for the assurance classes on which the person is authorized to work. Examples of the knowledge required by ISO/IEC 18045 are given in [Annex B](#).

Every evaluator working in the ALC class shall additionally have the following knowledge:

- c) site security (including physical, technical, organisational and personnel security requirements and measures, IT logical security/network security);
- d) site audits;
- e) secure development processes;
- f) software/hardware bill of materials;
- g) configuration management and development practices;
- h) information security standards; and
- i) methods for product development and its life cycle.

NOTE The class ALC is defined in ISO/IEC 15408-3.

4.1.3 Knowledge of the assurance paradigm

4.1.3.1 Knowledge of the evaluation scheme and overall evaluation framework

Evaluation schemes usually specify an overall evaluation framework with scheme-specific scope, regulations and application rules. Organizations implementing such an evaluation scheme as well as review bodies working within such an evaluation scheme typically define specifications based on the scheme. Within the predefined limits they also define their operational framework such as policies and procedures that are specific to the evaluation scheme.

Every evaluator shall be able to demonstrate knowledge of the evaluation schemes as required to fulfil their role according to their competence level. Applicable evaluation schemes are those in which the person is authorized to work.

Every evaluator shall have the necessary knowledge of the following items that are of relevance to the evaluation-related work on which the evaluator is authorized to work:

- a) scope of the evaluation scheme;
- b) any (sector-specific) regulations, legislation, policies, and further specifics;
- c) different types of evaluation/review procedures (e.g. initial review, assurance continuity as re-review, re-assessment, maintenance);
- d) guidance for organizations implementing evaluation schemes and to their evaluators;
- e) recognition arrangements;
- f) vulnerability disclosure and handling;
- g) scope of the implementing organization;
- h) policies regarding evaluation projects including entry criteria, time limits and site visit requirements;
- i) specific supporting documents;
- j) specific interpretations;
- k) specific guidance for evaluators;
- l) approved protection profiles and their supporting documents;
- m) specific assurance methods;
- n) reporting requirements;
- o) quality; and
- p) laboratory approval requirements.

NOTE See ISO/IEC 18045:—, A.5 for guidance on evaluation schemes on this topic.

4.1.3.2 Knowledge of the review body

Every evaluator shall be able to demonstrate knowledge of the review bodies, in order to fulfil their role according to their competence level. The applicable review bodies are those for which the person is authorized to work.

NOTE A review body is called an "evaluation authority" in ISO/IEC 15408-1.

EXAMPLE The Common Criteria Recognition Arrangement (CCRA) and the Senior Officials Group Information Systems Security (SOG-IS) are mutual recognition arrangements under which several evaluation schemes with their certification bodies for Common Criteria certification work. The European Union Common Criteria Scheme (EUCC) is an evaluation scheme itself with several assigned certification bodies.

Every evaluator shall have the necessary knowledge of the following items that are of relevance to the evaluation-related work on which the evaluator is authorized to work:

- a) scope of the review body;
- b) different types of evaluation/review procedures (e.g. initial review, assurance continuity as re-review, re-assessment, maintenance);
- c) review body policies;
- d) policies regarding to evaluation projects including entry criteria, time limits and site visit requirements;
- e) specific interpretations;
- f) specific supporting documents;
- g) specific guidance;
- h) specific assurance methods;
- i) reporting requirements;
- j) vulnerability disclosure and handling; and
- k) quality.

4.1.3.3 Knowledge of the laboratory and its management system

Every evaluator shall have the necessary knowledge of the following items in order to fulfil their role and in accordance with the requirements of the evaluation scheme:

- a) the laboratory's management system, including policies, processes and procedures that are applicable to evaluators;
- b) laboratory approved methods; and
- c) laboratory competence requirements.

NOTE Management systems vary greatly in their implementations. However, items such as document control, record control, control of nonconforming testing and calibration work, handling of technical records, and conflict of interest are often the direct responsibility of every evaluator. Most laboratory management systems are based on ISO/IEC 17025.

4.1.4 Knowledge of information security

Every evaluator shall have the necessary knowledge of the following concepts in order to fulfil their role and in accordance with the requirements of the evaluation scheme:

- a) security principles;
- b) security properties;
- c) mechanisms of attack;
- d) attack potential;
- e) cryptography;
- f) secure development lifecycles;
- g) security testing;
- h) vulnerabilities and weaknesses; and

- i) information security state-of-the-art concepts and technologies.

See [4.1.5](#) for further details on the information security topics outlined in a) to i) above, with which evaluators are expected to be familiar.

4.1.5 Knowledge of the technology

4.1.5.1 Knowledge of technology types

The ISO/IEC 15408 series and ISO/IEC 18045 can be used in the evaluation of a wide variety of information technologies. These technologies are often classified into various technology types by organizations implementing evaluation schemes, review bodies or others.

Every evaluator shall have the necessary knowledge of the information technology types on which the evaluators are authorized to work, including the common security architectures deployed for that technology type.

NOTE [Annex A](#) provides an informative list of knowledge topics presented by commonly identified technology types.

EXAMPLE Commonly identified technology types include:

- authenticator devices, access control devices and systems;
- encryption, key management and public key infrastructures (PKI) systems, products for digital signatures;
- databases;
- operating systems;
- network and network-related devices and systems;
- mobile devices and systems;
- multi-function devices;
- ICs, smart-cards and smart-card related devices and systems;
- hardware devices;
- detection devices and systems; and
- data protection, biometric systems and devices, trusted computing.

4.1.5.2 Knowledge of protection profiles, packages and supporting documents

Every evaluator shall have the necessary knowledge of the following, where applicable for the information technology on which the evaluator is authorized to work:

- a) protection profiles, functional packages, assurance packages, PP-Modules, PP-Configurations and any related supporting documents specified in connection with the evaluator's work;
- b) any additional evaluation methods and assurance activities specified as applicable to an evaluation; and
- c) how to determine if any interpretations or guidance in regard to protection profiles, packages and related supporting documents have been issued and whether they are applicable to a particular evaluation project.

Additionally, they may have knowledge of:

- d) documents that are specific to certain schemes; and

EXAMPLE 1 The EUCC documents for “IC, smartcards and similar devices” and “hardware devices with security boxes” technical domains.

- e) the cPP concept and specific cPPs.

EXAMPLE 2 cPPs for network security and operation system security.

4.1.5.3 Knowledge of specific technology

Since technology can vary and are continually evolving, it is not possible to identify all the knowledge required. [Annex A](#) provides a list of examples of both knowledge and skills for many technologies. Additional general guidance is provided in References [23] and [46], and examples for sector-specific guidance can be found in References [1],[5],[6] and [13].

Guidance on how to gain, maintain and update technology-related knowledge is provided in [A.3](#).

4.1.5.4 Knowledge for the evaluation of protection profiles, PP-Modules and PP-Configurations (classes APE and ACE)

Every evaluator evaluating protection profiles (PP) shall have additional knowledge, including the following:

- a) knowledge of the TOE's intended usage, surrounding system and processes, threat model, security objectives and provided security functionality;
- b) extensive knowledge of the relevant product type;
- c) specific knowledge of the technology used in the product type used in the PP, including the possibilities (and limitations) of this technology;
- d) knowledge on the operating environment of the product type;
- e) knowledge of the lifecycle of the product type;
- f) knowledge about modularization concepts like packages, modular PPs, conformance claims on other PPs, multi-assurance;
- g) knowledge of other PPs from the same domain;
- h) in depth knowledge of ISO/IEC 15408-2;
- i) knowledge of relevant cryptographic catalogues and standards; and
- j) modelling of algorithms, protocols and management functionality.

4.2 Knowledge required for reviewers

4.2.1 General

[4.2.2](#) to [4.2.5](#) address the knowledge that is required to review according to the ISO/IEC 15408 series and ISO/IEC 18045.

Some knowledge is required for every reviewer independent of their specific task, while other knowledge is required only depending on the specific review task and the TOE to which the reviewer is assigned.

NOTE The elements of knowledge that are required for competence can be enhanced by the previous experience gained through tasks related to the use of the ISO/IEC 15408 series and related documents. These tasks can include performing related work such as evaluation, consultancy, product development, research and specification of requirements.

4.2.2 Knowledge of the ISO/IEC 15408 series and ISO/IEC 18045

4.2.2.1 Generic knowledge of the ISO/IEC 15408 series and ISO/IEC 18045

Every reviewer's knowledge shall include:

- a) the terms and definitions defined in ISO/IEC 15408-1:—, Clause 3, ISO/IEC 15408-2:—, Clause 3 and ISO/IEC 15408-3:—, Clause 3 ;
- b) the terms and definitions defined in ISO/IEC 18045:—, Clause 3; and
- c) the context for evaluations of the ISO/IEC 15408 series.

4.2.2.2 Knowledge of ISO/IEC 15408-1

Every reviewer shall be able to demonstrate knowledge about the topics required to fulfil their role according to their competence level.

Every reviewer's knowledge shall include:

- a) the general model for the ISO/IEC 15408 series given in ISO/IEC 15408-1;
- b) tailoring security requirements: operations, dependencies between components and extended components;
- c) handling of review results;
- d) the specification of security targets;

When the reviewer's role and competency level demand it, their knowledge shall include some of the following:

- e) specification of protection profiles, modules, configurations and packages;
- f) composition models;
- g) multi-assurance-approach; and
- h) modularization concepts.

4.2.2.3 Knowledge of ISO/IEC 15408-2

Every reviewer shall be able to demonstrate knowledge about the security functional requirements (SFRs) of ISO/IEC 15408-2 required to fulfil their role according to their competence level and the technology types on which the reviewer is authorized to work, as well as any dependent SFRs. Examples of the knowledge required by ISO/IEC 15408-2 are given in [Annex C](#).

If the reviewer is required to demonstrate competence in ISO/IEC 15408-2, then knowledge of the respective security functional requirements shall be demonstrated.

4.2.2.4 Knowledge of ISO/IEC 15408-3

Every reviewer shall be able to demonstrate knowledge about the security assurance requirements (SARs) given in ISO/IEC 15408-3 required to fulfil their role according to their competence level and as specified by Security Targets (ST) on which the reviewer is authorized to work. Examples of the knowledge required by ISO/IEC 15408-3 are given in [Annex B](#).

If the reviewer is required to demonstrate competence in ISO/IEC 15408-3, then knowledge of the respective security assurance requirements shall be demonstrated.