INTERNATIONAL STANDARD

ISO/IEC 19896-3

First edition
2018-08

IT security techniques — Competence requirements for information security testers and evaluators —

Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

Techniques de sécurité IT — Exigences en matière de compétences des spécialistes en tests et évaluations de la sécurité de l'information —

Partie 3: Exigences en matière de connaissances, compétences et efficacité des spécialistes en évaluations ISO/IEC 15408

Reference number
ISO/IEC 19896-3:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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.

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 IT products and for assurance measures applied to these IT products during a security evaluation. Many certification and evaluation schemes as well as evaluation authorities 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.

One important factor in assuring comparability of the results of such evaluations is to understand that the evaluation process includes the specification of both objective and subjective assurance measures. Hence, the competence of the individual evaluators is important when the comparability and repeatability of evaluation results are the foundation for mutual recognition.

ISO/IEC 17025, provides general requirements for the competence of testing and calibration laboratories. In ISO/IEC 17025:2017, 5.2.1, it is stated that "*Personnel performing specific tasks shall be qualified on the basis of appropriate education, training, experience and/or demonstrated skills*".

This document establishes a baseline for the minimum competence of ISO/IEC 15408 evaluators with the goal of establishing conformity in the requirements for the training of ISO/IEC 15408 evaluator professionals associated with IT product evaluation schemes and authorities. It provides the specialized requirements to demonstrate the competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045. ISO/IEC 15408-1 describes the general framework for competences including the various elements of competence; knowledge, skills, experience, education and effectiveness. This document includes knowledge and skills especially in the following areas.

— Information security

  Knowledge: Information security principles, information security properties, information security threats and vulnerabilities

  Skills: Understand information security requirements, understand the context

— Information security evaluation

  Knowledge: Knowledge of ISO/IEC 15408 (all parts) 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: Understand 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: Create and manage an information security test plan, design information security tests, prepare and conduct information security tests

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

IT security techniques — Competence requirements for information security testers and evaluators —

Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

1 Scope

This document provides the specialized requirements to demonstrate competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045.

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, *IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19896-1, ISO/IEC 15408-1, ISO/IEC 17025, ISO/IEC 18045 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
evaluation scheme
organization implementing policies and a set of rules established by an evaluation authority, defining the evaluation environment, including criteria and methodology required to conduct IT security evaluations

3.2
subjective method
method based on a given person's experience, and understanding

4 Knowledge

4.1 General

Knowledge is what an evaluator knows and can describe. Subclauses 4.2 to 4.8 address the knowledge that is needed for evaluation to ISO/IEC 15408 (all parts) and ISO/IEC 18045.

4.2 Knowledge of ISO/IEC 15408 and ISO/IEC 18045

4.2.1 ISO/IEC 15408-1

All evaluators shall have knowledge of:

a) the terms and definitions defined in ISO/IEC 15408-1;

b) the terms and definitions defined in ISO/IEC 18045;

c) the context for ISO/IEC 15408 evaluations;

d) the general model for the ISO/IEC 15408 series given in ISO/IEC 15408-1;

e) tailoring security requirements: operations, dependencies between components and extended components;

f) protection profiles and packages;

g) evaluation results; and

h) the specification of security targets.

4.2.2 ISO/IEC 15408-2

All evaluators shall have knowledge of those security functional requirements (SFRs) of ISO/IEC 15408-2 which are used for the technology types the evaluator is authorized to work with, as well as any dependent SFRs. The classes of SFRs given in ISO/IEC 15408-2 are:

a) security audit (FAU);

b) communication (FCO);

c) cryptographic support (FCS);

d) user data protection (FDP);

e) identification and authentication (FIA);

f) security management (FMT);

g) privacy (FPR);

h) protection of the target of evaluation security functions (FPT);

i) resource utilisation (FRU);

j) target of evaluation access (FTA); and

k) trusted path/channels (FTP).

4.2.3 ISO/IEC 15408-3

All evaluators shall have knowledge of the security assurance requirements (SARs) given in ISO/IEC 15408-3 which are specified by Security Targets (ST) that the evaluator is authorized to work with.

The knowledge of particular SAR components shall include those to which the evaluator is authorized to work at. The classes of SARs given in ISO/IEC 15408-3 are:

a) development (ADV);

b) guidance documentation (AGD);

c) life-cycle support (ALC);

d) security target structure (ASE);

e) protection profile structure (APE);

f) tests (ATE);

g) vulnerability assessment (AVA); and

h) composition (ACO).

4.2.4 ISO/IEC 18045

All evaluators shall have knowledge of:

a) the evaluation process: this process is described in ISO/IEC 18045:2008, Clause 8; and

b) security evaluation method and activities: this information is given in ISO/IEC 18045.

4.3 Knowledge of the assurance paradigm

4.3.1 Knowledge of the evaluation authority

All evaluators shall have knowledge of the requirements of the evaluation authority or evaluation authorities that are applicable to the evaluation schemes for which they are authorized to work.

NOTE Examples of such evaluation authorities include "Common Criteria Recognition Agreement (CCRA)" and the "Senior Officials Group Information Systems Security (SOG-IS)".

Requirements from evaluation authorities can include topics such as:

a) the scope of the evaluation authority;

b) recognition arrangements;

c) evaluation authority policies;

d) guidance to evaluation schemes, validators and evaluators;

e) interpretations;

f) supporting documents;

g) knowledge of related standards; and

h) quality requirements.

4.3.2 Knowledge of the evaluation scheme

Evaluation schemes typically define operational aspects such as policies, and procedures that are specific to the evaluation scheme. Such items are often based on the scope of the evaluation scheme.

All evaluators shall have knowledge of:

a) The requirements of the evaluation scheme or schemes for which they are authorized to work;

EXAMPLE

— any sector specific policies, regulations and legislation;

— laboratory approval requirements for the evaluation scheme;

— evaluation scheme policies in regard to evaluation projects including entry criteria, time limits, report requirements, site visit requirements;

— guidance to validators and evaluators;

— evaluation scheme specific interpretations;

— evaluation scheme specific guidance;

— approved protection profiles and their supporting documents;

— evaluation scheme specific assurance methods and activities; and

— reporting requirements.

b) the competence requirements of the evaluation scheme for evaluators.

NOTE See ISO/IEC 18045:2008, A.5 for guidance to evaluation schemes on this topic.

4.3.3 Knowledge of the laboratory and it's management system

All evaluators shall have knowledge of:

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/or calibration work, handling of technical records, and conflict of interest are often the direct responsibility of evaluators. Most laboratory management systems are based on ISO/IEC 17025.

4.4 Knowledge of information security

All evaluators shall have knowledge of:

a) security principles;

b) security properties;

c) mechanisms of attack;

d) concepts of attack potential;

e) secure development life cycles;

f) security testing; and

g) vulnerabilities and weaknesses.

4.5 Knowledge of the technology being evaluated

4.5.1 Knowledge of the technology being evaluated

ISO/IEC 15408 (all parts) 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 evaluation schemes, evaluation authorities or others.

All evaluators shall have knowledge of the information technology types being evaluated by them, 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:

— access control devices and systems;

— encryption, key management and 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.

4.5.2 Protection Profiles, packages and supporting documents

All evaluators shall have knowledge of the following, where they are applicable for the information technology evaluated by them:

a) protection profiles, packages and any related supporting documents specified in connection with the evaluator's work;

b) the knowledge required to meet any additional evaluation methods and assurance activities specified as applicable to an evaluation;

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.

4.6 Knowledge required for specific assurance classes

Evaluators need the knowledge required by the evaluation methods and activities specified for the assurance classes for which they are authorized to work. Examples for the knowledge required by ISO/IEC 18045 are given in Annex B.

4.7 Knowledge required when evaluating specific security functional requirements

Evaluators shall have the knowledge required as given by the security functional requirements they are authorized to evaluate as specified in ISO/IEC 15408-2. Examples for the knowledge required by ISO/IEC 15408-2 are given in Annex C.

4.8 Knowledge needed when evaluating specific technologies

Since technology can vary and are continually evolving it is not possible to identify all the skills required. Annex A provides an informative list of both knowledge and skills for many technologies. In addition, the Bibliography gives many technology related references.

Technology related knowledge can be obtained through experience with that technology. Such experience can be developed by:

a) participating in education in regard to the technology;

b) working as a trainee alongside an experienced evaluator;

c) working in the development of the technology; and

d) performing research on the technology.

5 Skills

5.1 Basic evaluation skills

5.1.1 Evaluation methods

All evaluators shall have skills in basic evaluation methods. These include both objective and subjective methods, including:

a) sampling;

b) basic statistical analysis;

c) observation;

d) analysis;

e) comparison; and

f) recording results;

5.1.2 Evaluation tools

The evaluator shall be skilled in:

a) the use of tools that are specified by the laboratory or evaluation scheme in support of evaluation, report generation, delivery or protection of documents and results;

EXAMPLE

— encryption tools; and

— documentation tools.

b) specialized tools for certain evaluation tasks as specified by the laboratory or evaluation scheme or supporting documents.

EXAMPLE

— specialized mathematical tools for analysing measured data;

— tools for verifying implementation of crypto algorithms.

5.2 Core evaluation skills given in ISO/IEC 15408-3 and ISO/IEC 18045

5.2.1 Evaluation principles

All evaluators shall be able to perform their work in a way that is:

a) impartial;

b) objective;

c) repeatable; and

d) reproducible.

5.2.2 Evaluation methods and activities

All evaluators shall have skills in the core evaluation methods and activities specified in ISO/IEC 18045, Protection Profiles and any supporting documents.

The following verbs have special meaning in ISO/IEC 18045:2008 and the evaluator shall be skilled in performing the activities in accordance with the definitions made in ISO/IEC 18045:2008. These are expressed as the following verbs:

a) check;

b) confirm;

c) demonstrate;

d) describe;

e) determine;

f) ensure;

g) be exhaustive;

h) examine;

i) explain;

j) justify;

k) prove;

l) report;

m) record;

n) specify;

o) trace; and

p) verify.

NOTE These terms are defined and explained in either ISO/IEC 15408-1 or ISO/IEC 18045:2008.

5.3 Skills required when evaluating specific security assurance classes

5.3.1 General

Evaluators performing evaluation activities shall be able to write observation reports.

The further skills required are listed for each class in Tables 1 to 7. Within each family, the skills required increase both in depth and width. The additional skills are listed in higher members of the family while the increased depth of the skills is not explicitly mentioned but shall be considered when authorizing evaluators.

EXAMPLE 1 An evaluator who is authorized to evaluate ADV_FSP.2 needs to be able to check tracing links of the SFRs before obtaining authorization for ADV_FSP.3.

EXAMPLE 2 For ADV_TDS.1, only basic skills regarding TOE architecture are required, while for ADV_TDS.6, skills to handle formal methods for the architecture are required.

5.3.2 ADV (Development) Class

Evaluators performing evaluation activities related to the ADV class shall have the skills identified in Table 1 for the assurance components up to and including the component that they are evaluating.

Table 1 — Skills required for ADV class evaluators

Assurance component	Evaluation skills required
ADV_ARC.1	a) Being able to cross-check architectural information with other evidence provided for the evaluation.
ADV_FSP.1	a) Being able to identify program and application interfaces; b) Being able to determine the TSFIs.
ADV_FSP.2	No additional requirements.
ADV_FSP.3	c) Being able to check tracing links of the SFRs;
ADV_FSP.4	No additional requirements.
ADV_FSP.5	d) Being able to understand semi-formal language;
ADV_FSP.6	e) Being able to understand formal language; f) Being able to verify the correctness of the formal model and also the completeness of the reasoning.
ADV_IMP.1	a) Use of sampling techniques; b) Being able to read and understand source code or hardware diagrams and/ or IC hardware design language code or layout data used in implementing the TOE; c) Being able to use tools allowing for un-shrouding or de-obfuscation; d) Being able to understand generation tools, their usage, and their effects. EXAMPLE Compiler configurations.
ADV_IMP.2	No additional requirements.
ADV_INT.1	No additional requirements.
ADV_INT.2	a) Being able to identify standards relevant to the TSF in order to determine if the TSF is well-structured;
ADV_INT.3	b) Being able to judge the complexity of the TSF internals;
ADV_SPM.1	a) Being able to understand the security policy model and determine if it is complete;
ADV_TDS.1	a) Being able to understand the architecture of the TOE.

Table 1 *(continued)*

Assurance component	Evaluation skills required
ADV_TDS.2	No additional requirements.
ADV_TDS.3	No additional requirements.
ADV_TDS.4	No additional requirements.
ADV_TDS.5	No additional requirements.
ADV_TDS.6	No additional requirements.

5.3.3 AGD (Guidance Documents) Class

Evaluators performing evaluation activities related to the AGD class shall have the skills identified in Table 2 for the assurance components that they are evaluating.

Table 2 — Skills required for AGD class evaluators

Assurance component	Evaluation skills required
AGD.OPE.1	a) Being able to understand that the operation is correct and secure according to the evidence;
AGD_PRE.1	a) Being able to understand that the installation is correct and secure according to the evidence;

5.3.4 ALC (Life-Cycle Support) Class

Evaluators performing evaluation activities related to the ALC class shall have the skills identified in Table 3 for the assurance components that they are evaluating.

Table 3 — Skills required for ALC class evaluators

Assurance component	Evaluation skills required
ALC_CMC.1	a) Being able to observe the use of the CM system as described in the CM plan;
ALC_CMC.2	No additional requirements.
ALC_CMC.3	No additional requirements.
ALC_CMC.4	No additional requirements.
ALC_CMC.5	No additional requirements.
ALC_CMS.1	a) Being able to understand versioning and identification schema; b) Being able to determine if configuration items are uniquely identified.
ALC_CMS.2	No additional requirements.
ALC_CMS.3	No additional requirements.
ALC_CMS.4	No additional requirements.
ALC_CMS.5	No additional requirements.
ALC_DEL.1	a) Being able to follow written delivery and installation procedures.
ALC_DVS.1	a) Site visit planning; b) On-site and personnel assessment techniques; c) Being able to observe the application of security measures during development and maintenance of the TOE as described in the development security documentation; d) Being able to observe the practical application of delivery procedures as described in the delivery documentation.

Table 3 *(continued)*

Assurance component	Evaluation skills required
ALC_DVS.2	No additional requirements.
ALC_FLR.1	a) Being able to understand flaw remediation processes.
ALC_FLR.2	No additional requirements.
ALC_LCD.1	a) Being able to analyse the life cycle processes presented by the developer.
ALC_LCD.2	No additional requirements.
ALC_TAT.1	a) Being able to analyse the tools and techniques presented by the developer.
ALC_TAT.2	No additional requirements.
ALC_TAT.3	No additional requirements.

5.3.5 ASE and APE (ST and PP evaluation) Classes

Evaluators performing evaluation activities related to the ASE class shall have the skills identified in Table 4 for the assurance components that they are evaluating.

Table 4 — Skills required for ASE and APE class evaluators

Assurance component		Evaluator skills required
ASE_CCL.1	APE_CCL.1	a) Being able to check that the conformance claim is correct.
ASE_ECD.1	APE_ECD.1	a) Being able to understand that the extended components definition is correct.
ASE_INT.1	APE_INT.1	a) Being able to understand that the introduction describes the TOE and the TOE context correctly.
ASE_OBJ.1	APE_OBJ.1	a) Being able to determine if the security objectives adequately and completely address the security problem definition; b) Being able to determine if the security objectives are properly divided between security objectives of the TOE and the security objectives for the TOE environment correctly and together address the security problem definition.
ASE_OBJ.2	APE_OBJ.2	No additional requirements.
ASE_REQ.1	APE_REQ.1	a) Being able to determine that the security requirements are clear, unambiguous and well-defined.
ASE_REQ.2	APE_REQ.2	No additional requirements.
ASE_SPD.1	APE_SPD.1	a) Being able to understand that the security problem definition is correct.
ASE_TSS.1		a) Being able to map narrative to specific SFRs.

5.3.6 ATE (Tests) Class

Evaluators performing evaluation activities related to the ATE class shall have the skills identified in Table 5 for the assurance components that they are evaluating.

Table 5 — Skills required for ATE class evaluators

Assurance component	Evaluator skills required
ATE_COV.1	a) Being able to understand the test coverage presented; b) Being able to understand tests and verify that the results of tests are correct;
ATE_COV.2	No additional requirements.
ATE_COV.3	No additional requirements.
ATE_DPT.1	a) Being able to understand the test coverage documentation provided by the developer; b) Being able to understand testing at a subsystem level.
ATE_DPT.2	a) Being able to understand testing at a module level.
ATE_DPT.3	No additional requirements.
ATE_DPT.4	No additional requirements.
ATE_FUN.1	a) Being able to understand the functional testing documentation provided by the developer.
ATE_FUN.2	No additional requirements.
ATE_IND.1	a) Development of a test plan; b) Development of appropriate test cases; c) Configuration of the TOE; d) Setup and configuration of the TOE environment; e) Maintaining the integrity of the test environment; f) Configuring and using test tools specified in the test plan; g) Commissioning appropriate test harnesses and test scripts. NOTE This can include the use of programming languages, scripting languages, and debug facilities.
ATE_IND.2	No additional requirements.
ATE_IND.3	No additional requirements.

5.3.7 AVA (Vulnerability Assessment) Class

Evaluators performing evaluation activities related to the AVA class shall have the skills identified in Table 6 for the assurance components that they are evaluating.

Table 6 — Skills required for AVA class evaluators

Assurance component	Evaluator skills required
AVA_VAN.1	a) Being able to identify appropriate keywords for a vulnerability search; b) Being able to identify appropriate sources of information for publically known vulnerabilities for a particular TOE; c) Being able to understand the evidence of vulnerabilities analysis and verify that the result of the evidence is correct; d) Being able to analyse cause and effect relationships of TOE functionality; e) Being able to identify residual vulnerabilities; f) Being able to calculate the attack potential.
AVA_VAN.2	No additional requirements
AVA_VAN.3	g) Flaw hypothesis development;
AVA_VAN.4	No additional requirements.
AVA_VAN.5	No additional requirements.

5.3.8 ACO (Composition) Class

Evaluators performing evaluation activities related to the ACO class shall have the skills identified in Table 7 for the assurance components that they are evaluating.

Table 7 — Skills required for ACO class evaluators

Assurance component	Evaluator skills required
ACO_COR.1	No additional requirements.
ACO_DEV.1	No additional requirements.
ACO_DEV.2	No additional requirements.
ACO_DEV.3	No additional requirements.
ACO_REL.1	No additional requirements.
ACO_REL.2	No additional requirements.
ACO_CTT.1	a) The skills identified for the ADV_FSP class given in Table 1;
ACO_CTT.2	No additional requirements.
ACO_VUL.1	a) The skills identified for the AVA_VAN class given in Table 6; b) Being able to determine if the assumptions and objectives specified for the each of the components operational environment, remains true for a composed TOE; c) Being able to identify vulnerabilities introduced as a result of composition; d) Being able to perform penetration testing.
ACO_VUL.2	No additional requirements.
ACO_VUL.3	No additional requirements.

5.4 Skills required when evaluating specific security functional requirement classes

5.4.1 General

For each class, the evaluator shall be able to:

a) understand and test for conformance to related technological standards; and

b) search for potential vulnerabilities and side channels.

5.4.2 Skills required when evaluating the FCS (Cryptographic support) Class

a) being able to determine if cryptographic algorithms and protocols are implemented correctly.

5.5 Skills needed when evaluating specific technologies

Since technology can vary and are continually evolving it is not possible to identify all the skills required. Annex A provides a list of both knowledge and skills for some technologies.

Technology related skills can be obtained through experience with that technology. Such experience can be developed by:

a) attending skills-training related to the technology;

b) working as a trainee alongside an experienced evaluator;

c) working in the development of such technologies; and

d) performing research on the technology.

6 Experience

Experience in the core evaluation skills, given in Clause 5, is gained during the first and subsequent evaluations performed by an evaluator. As a trainee, such experience should be gained under the supervision and/or mentorship of another competent evaluator.

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

7 Education

All evaluators should have a tertiary educational qualification, such as an Associate, Bachelor's, or higher degree, that is relevant to the requirements addressed in ISO/IEC 15408 and the evaluation methodology requirements in ISO/IEC 18045.

All evaluators shall, at a minimum, demonstrate they have either:

a) successfully completed appropriate tertiary education with at least 3 years of study in disciplines including specific technical specialities related to IT or IT security; or

b) had experience which provided equivalent knowledge, skills and effectiveness to that gained through tertiary education in disciplines related to IT or IT security.

EXAMPLE Examples of specific technical specialities include:

— engineering technology;

— electrical engineering;

— mechanical engineering;

— material engineering;

— computer information technology;

— computer engineering;

— computer science;

— computer networks;

— cybersecurity;

— physics;

— formal mathematics;

— information systems; and

— software development and security.

8 Effectiveness

8.1 General

The evaluator shall be able to apply knowledge and skills in a productive manner, characterized by attributes of behaviour such as aptitude, initiative, enthusiasm, willingness, communication skills, team participation, and leadership.

8.2 Effectiveness of the evaluation

Subclause 5.2.1, lists the evaluation principles that are required to be followed in order to achieve an effective evaluation.

8.3 Evaluation scheme responsibilities for evaluator effectiveness

ISO/IEC 18045:2008, A.5 provides guidance to evaluation schemes on their expected responsibilities. Many items related are directly or indirectly related to evaluator effectiveness and should be considered by evaluation facilities when determining effectiveness.

8.4 Effectiveness in performing timely evaluations

Measurement criteria for the effectiveness of evaluators are found ISO/IEC 19896-1:2018, 8.5.

8.5 Effectiveness in performing accurate evaluations

All evaluators shall be able to perform assigned evaluation tasks that follow defined evaluation methods and activities with accuracy.

8.6 Effectiveness in reporting results

All evaluators shall be able to express the results of the evaluation so that the rationale for the decision and the references to the relevant documents are quickly understandable by the intended reader of the report.

Annex A
(informative)

Technology types: Knowledge and skills

A.1 Knowledge related to specific technology types

A.1.1 General

The taxonomy of technology types varies according to the needs of those entities categorizing them. The technology types presented in A.1 are those that are frequently used, the reader is to be aware that other technology types can be identified.

The depth of knowledge required by an evaluator varies depending on the security requirements which they evaluate. Evaluators engaged with ADV, ASE and APE, ATA, AVA and ACO assurance classes need a greater depth of knowledge then those evaluating the ALC class. In general, evaluators engaged with the evaluation of security functional requirements will need to understand the technology employed. However, depending on the evaluation methods and activities specified, this may not be necessary.

The following knowledge is identified as being needed by evaluators working with specific technology types:

a) PPs related to the technology type;

b) evaluation methods and activities related to the technology type; and

c) technological standards related to the technology type.

A.1.2 Access control devices and systems

a) access control methods.

A.1.3 Biometric systems and devices

a) statistical techniques; and

b) biometric modalities.

A.1.4 Data protection

a) databases;

b) scanning techniques; and

c) intrusion detection.

A.1.5 Databases

a) concepts of data base management systems architecture; and

b) access control methods.

A.1.6 Detection devices and systems

a) concepts of detection devices and systems architecture; and

b) concepts of pattern recognition.

A.1.7 ICs, smart-cards and smart-card related devices and systems

a) concepts of smart card architecture;

b) smart card readers and their drivers;

c) crypto processors;

d) secure key storage;

e) wired/wireless interfaces;

f) physical true random bit generator;

g) concepts of tamper proofing, resistance, detection, evidence, response; and

h) side channel analysis.

A.1.8 Hardware devices

a) physical security;

b) concepts of tamper proofing, resistance, detection, evidence, response; and

c) side channel analysis.

A.1.9 Key management systems

a) key management methods and techniques;

b) random number generation;

c) concepts of entropy;

d) key generation;

e) key establishment;

f) key entry and output;

g) key storage;

h) key zeroization; and

i) key transport.

A.1.10 Mobile devices and systems

a) concepts of mobile device architecture; and

b) concepts of mobile device management.

A.1.11 Multi-function devices

a) concepts of multi-function device architecture.

A.1.12 Network and network-related devices and systems

a) network architectures and topologies; and

b) commonly used network protocols.

A.1.13 Operating systems

a) secure boot;

b) protection rings,

c) memory management;

d) least privilege principle;

e) access control mechanisms;

f) principles of virtualization;

g) separation; and

h) deterministic RBG.

A.1.14 Products for digital signatures

a) digital signature technologies;

b) public key infrastructures (PKI);

c) certificate authorities (CA); and

d) key generation algorithms.

EXAMPLE RSA, DSA and ECDSA.

A.1.15 Trusted computing

a) key trusted computing technology concepts.

1) trusted platform module keys such as endorsement key (EK) and storage root key (SRK);

2) platform configuration registers;

3) secure input and output;

4) memory curtaining;

5) sealed storage; and

6) remote attestation.

A.2 Skills related to specific technology types

A.2.1 General

When considering the skills required for certain technology types, the specific skills needed are mostly related to the ATE (testing) for that technology type. These skills build upon the basic skills that are defined within this document.

The following skills are identified as needed by evaluators working with specific technology types:

a) the performance of evaluation methods and activities associated with the technology type; and

b) being able to understand related technological standards.

A.2.2 Access control devices and systems

a) being able to install access control devices and systems.

A.2.3 Biometric systems and devices

a) use of statistical techniques.

A.2.4 Data protection

a) being able to install access control devices and systems.

A.2.5 Databases

a) being able to correctly configure the database management system (DBMS) platforms; and

b) being able to use structured query language (SQL) or other database query languages.

A.2.6 Detection devices and systems

a) being able to install and configure detection devices and systems.

A.2.7 ICs, smart cards and smart card-related devices and systems

a) being able to install smart-card readers and their drivers on test platforms;

b) being able to prepare integrated circuits for testing;

EXAMPLE The use of probes.

c) being able to configure and use electronics testing equipment;

EXAMPLE Oscilloscopes, protocol analyser.

d) being able to configure and use emulators and simulators;

e) use of physical security techniques for penetration testing; and

f) being able to initiate and perform side-channel attacks.

A.2.8 Hardware devices

a) use of physical security techniques for penetration testing;

b) being able to initiate and perform side-channel attacks;

c) being able to configure and use electronics testing equipment; and

EXAMPLE Oscilloscopes, protocol analysers.

d) being able to configure and use emulators and simulators.

A.2.9 Key Management systems

No specialized skills for this technology type have been identified.

A.2.10 Mobile devices and systems

No specialized skills for this technology type have been identified.

A.2.11 Multi-function devices

No specialized skills for this technology type have been identified.

A.2.12 Network and network-related devices and systems

No specialized skills for this technology type have been identified.

A.2.13 Operating systems

a) being able to identify an operating system's TOE security function interface (TSFI).

A.2.14 Products for digital signatures

No specialized skills for this technology type have been identified.

A.2.15 Trusted computing

No specialized skills for this technology type have been identified.

Annex B
(informative)

Examples of knowledge required for evaluating security assurance requirement classes

This annex contains examples of the knowledge required by evaluators for the evaluation of the security assurance requirement classes given in ISO/IEC 15408-3. The examples are based on the evaluation methodology given in ISO/IEC 18045.

B.1 Knowledge required for specific assurance classes

B.1.1 ADV (Development) Class

Evaluators performing evaluation activities related to the ADV class should have the knowledge identified in Table B.1, up to and including the level of detail of the assurance components in their assigned area of evaluation responsibility.

Table B.1 — Knowledge required for ADV class evaluators

Assurance component	Minimum knowledge required
ADV_ARC.1	a) Self-protection property; b) Domain separation property; c) Non-bypassability property; d) Secure architecture and design concepts.
ADV_FSP.1	a) Concept of an interface; b) Concept of SFR-supporting and SFR-enforcing TSFI; c) Methods of the specification of program interfaces.
ADV_FSP.2	d) Security architecture; e) Error messages.
ADV_FSP.3	f) Parameters.
ADV_FSP.4	No additional requirements.
ADV_FSP.5	g) Formal security policy model; h) Semiformal style; i) A standardized format with a well-defined syntax; j) Structured presentation methods (pseudo-code, flow charts, block diagrams).
ADV_FSP.6	No additional requirements.
ADV_IMP.1	a) Sampling techniques; b) Source code languages or hardware diagram specification and/ or IC hardware design language code or layout data used in implementing the TOE; c) Shrouding or obfuscation techniques; d) Compilers.

Table B.1 *(continued)*

Assurance component	Minimum knowledge required
ADV_IMP.2	e) Evaluation scheme provided guidance; f) Techniques of generating TSF from an implementation representation (e.g. Compilers, interpreters).
ADV_INT.1	a) Internal structuring; b) Complexity.
ADV_INT.2	No additional requirements.
ADV_INT.3	No additional requirements.
ADV_SPM.1	a) Formal security policy models including an understanding of policies for access control, audit, identification, authentication, encryption, and management; b) Security architectures; c) Formal methods.
ADV_TDS.1	a) Levels of decomposition; b) Subsystem concepts and description including categorization, purpose, behaviour, interactions, interfaces; c) Module concepts and description including categorization, purpose, behaviour, interactions, interfaces; d) Concepts of SFR-enforcing, SFR-supporting and SFR-non-interfering.
ADV_TDS.2	No additional requirements.
ADV_TDS.3	No additional requirements.
ADV_TDS.4	No additional requirements.
ADV_TDS.5	e) Semiformal design description;
ADV_TDS.6	f) Proofs of correspondence.

B.1.2 AGD (Guidance Documents) Class

Evaluators performing evaluation activities related to the AGD class should have the knowledge identified in Table B.2, up to and including the level of detail of the assurance components in their assigned area of evaluation responsibility.

Table B.2 — Knowledge required for AGD class evaluators

Assurance component	Minimum knowledge required
AGD.OPE.1	a) Concepts of user roles; b) Concepts of groups; c) The user-accessible functions and privileges; d) Secure operation; e) Operational environment.
AGD_PRE.1	a) Delivery procedures; b) Secure installation techniques; c) Secure configuration.

B.1.3 ALC (Life-Cycle Support) Class

Evaluators performing evaluation activities related to the ALC class should have the knowledge identified in Table B.3, up to and including the level of detail of the assurance components in their assigned area of evaluation responsibility.

Table B.3 — Knowledge required for ALC class evaluators

Assurance component	Minimum knowledge required
ALC_CMC.1	a) Product life-cycle; b) Concepts of configuration management; c) Concepts of development security; d) Typical tools and techniques used in TOE development; e) Patching and flaw remediation processes; f) Integration and acceptance processes; g) Delivery processes; h) Build process (the process of transforming an implementation representation into the TOE); i) Concepts of configuration management; j) Commonly used configuration management systems; k) The application of configuration management, ensuring that the integrity of the TOE is preserved; l) Measures, procedures, and standards concerned with secure delivery of the TOE, ensuring that the security protection offered by the TOE is not compromised during the transfer to the user.
ALC_CMC.2	m) Configuration management systems security (access control);
ALC_CMC.3	n) Concepts of a configuration management system plan;
ALC_CMC.4	o) Configuration management acceptance procedures;
ALC_CMC.5	No additional requirements.
ALC_CMS.1	a) Concepts of configuration management; b) Commonly used configuration management systems.
ALC_CMS.2	No additional requirements.
ALC_CMS.3	No additional requirements.
ALC_CMS.4	No additional requirements.
ALC_CMS.5	No additional requirements.
ALC_DEL.1	a) Measures, procedures, and standards concerned with secure delivery of the TOE, ensuring that the security protection offered by the TOE is not compromised during the transfer to the user site; b) Tamper techniques including tamper proofing, resistance, detection and evidence.

Table B.3 *(continued)*

Assurance component	Minimum knowledge required
ALC_DVS.1	a) Security measures, used to protect the development environment including: 1) Security controls; 2) Physical security; 3) Personnel security; 4) Procedural security.
ALC_DVS.2	No additional requirements.
ALC_FLR.1	a) Methods of flaw remediation; b) Security flaw reporting in each stage of development; c) Patching and flaw remediation processes; d) Secure distribution of patches and changes.
ALC_FLR.2	e) Corrective action.
ALC_LCD.1	a) Development life cycle models EXAMPLE 1) Agile; 2) Waterfall. 3) Life-cycle input and output documentation.
ALC_LCD.2	No additional requirements.
ALC_TAT.1	a) Tools and techniques used in product development, including: 1) Well-defined development tools; EXAMPLE Programming languages or computer-aided design (CAD) systems, and 2) Implementation standards.
ALC_TAT.2	No additional requirements.
ALC_TAT.3	No additional requirements.

B.1.4 ASE & APE (ST and PP evaluation) Classes

Evaluators performing evaluation activities related to the ASE and APE classes should have the knowledge identified in Table B.4, up to and including the level of detail of the assurance components in their assigned area of evaluation responsibility.

Table B.4 — Knowledge required for ASE and APE class evaluators

Assurance component		Minimum knowledge required
ASE_CCL.1	APE_CCL.1	a) PP, ST, security requirement packages; b) Conformance claim.
ASE_ECD.1	APE_ECD.1	a) Being able to review definition of an extended component for each extended security requirement; b) Being able to review demonstration of conformance or non-conformance to these elements.
ASE_INT.1	APE_INT.1	No additional requirements.

Table B.4 *(continued)*

Assurance component		Minimum knowledge required
ASE_OBJ.1	APE_OBJ.1	a) Operational environment.
ASE_OBJ.2	APE_OBJ.2	No additional requirements.
ASE_REQ.1	APE_REQ.1	a) Subjects; b) Objects; c) Operations; d) Security attributes; e) External entities.
ASE_REQ.2	APE_REQ.2	No additional requirements.
ASE_SPD.1	APE_SPD.1	a) Security problem definition; b) Security objectives. c) Assets; d) Threats; e) Threat agent.
ASE_TSS.1	—	No additional requirements

B.1.5 ATE (Tests) Class

Evaluators performing evaluation activities related to the ATE class should have the knowledge identified in Table B.5, up to and including the level of detail of the assurance components in their assigned area of evaluation responsibility.

Table B.5 — Knowledge required for ATE class evaluators

Assurance component	Minimum knowledge required
All components	a) Concept of a test plan; 1) Resources required for testing; 2) Commonly used testing tools; 3) Test prerequisites; 4) Testing environment; 5) Test steps (test scenario); 6) Expected result of tests; 7) Recording methods of actual test results; 8) Test verdict. b) Common test methods (e.g., functional specification, toe design, module, etc.).
ATE_COV.1	a) Concepts of test coverage.
ATE_COV.2	No additional requirements.
ATE_COV.3	No additional requirements.
ATE_DPT.1	a) Concepts of depth of testing and link with subsystem.
ATE_DPT.2	b) Concepts of depth of testing and link with module.

Table B.5 *(continued)*

Assurance component	Minimum knowledge required
ATE_DPT.3	No additional requirements.
ATE_DPT.4	No additional requirements.
ATE_FUN.1	a) Concepts of functional testing;
ATE_FUN.2	No additional requirements.
ATE_IND.1	a) Type of interfaces (e.g. Programmatic, command-line, protocol); b) Development of flaw hypotheses; c) Testing techniques; d) Black and white box testing techniques.
ATE_IND.2	e) Sampling techniques; f) Development of independent test cases.
ATE_IND.3	No additional requirements

B.1.6 AVA (Vulnerability Assessment) Class

Evaluators performing evaluation activities related to the AVA class should have the knowledge identified in Table B.6, up to and including the level of detail of the assurance components in their assigned area of evaluation responsibility.

Table B.6 — Knowledge required for AVA class evaluators

Assurance component	Minimum knowledge required
AVA_VAN.1	a) Classification of vulnerabilities; b) Attack taxonomies; c) Identification of sources of public vulnerability information; d) Penetration testing.
AVA_VAN.2	No additional requirements.
AVA_VAN.3	e) Development of flaw hypotheses.
AVA_VAN.4	f) Evaluation scheme specific methods, tools and techniques.
AVA_VAN.5	No additional requirements.

B.1.7 ACO (Composition) Class

Evaluators performing evaluation activities related to the ACO class should have the knowledge identified in Table B.7, up to and including the level of detail of the assurance components in their assigned area of evaluation responsibility.

Table B.7 — Knowledge required for ACO class evaluators

Assurance component	Minimum knowledge required
All ACO components	a) Principles of composition; b) Types of composition; 1) Layering; 2) Network; 3) Component. c) Principles of system integration; d) Principles of reliance.
ACO_COR.1	No additional requirements.
ACO_DEV.1	a) Knowledge required for ADV class;
ACO_DEV.2	No additional requirements.
ACO_DEV.3	No additional requirements.
ACO_REL.1	a) Component interactions; b) Concept of reliance; c) Tamper protection techniques including tamper proofing, resistance, detection and evidence; d) Interference protection techniques.
ACO_REL.2	No additional requirements
ACO_CTT.1	a) Knowledge required for ATE class; b) Composed TOE testing;
ACO_CTT.2	No additional requirements.
ACO_VUL.1	a) Knowledge required for the AVA class; b) Knowledge of vulnerabilities applicable to composition; c) Information flow.
ACO_VUL.2	No additional requirements
ACO_VUL.3	No additional requirements