

ISO/IEC 19896-3:2018 (E)

IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Knowledge
4.1	General
4.2	Knowledge of ISO/IEC 15408 and ISO/IEC 18045
4.2.1	ISO/IEC 15408-1
4.2.2	ISO/IEC 15408-2
4.2.3	ISO/IEC 15408-3
4.2.4	ISO/IEC 18045
4.3	Knowledge of the assurance paradigm
4.3.1	Knowledge of the evaluation authority
4.3.2	Knowledge of the evaluation scheme
4.3.3	Knowledge of the laboratory and its management system
4.4	Knowledge of information security
4.5	Knowledge of the technology being evaluated
4.5.1	Knowledge of the technology being evaluated
4.5.2	Protection Profiles, packages and supporting documents
4.6	Knowledge required for specific assurance classes
4.7	Knowledge required when evaluating specific security functional requirements
4.8	Knowledge needed when evaluating specific technologies
5	Skills
5.1	Basic evaluation skills
5.1.1	Evaluation methods
5.1.2	Evaluation tools
5.2	Core evaluation skills given in ISO/IEC 15408-3 and ISO/IEC 18045
5.2.1	Evaluation principles
5.2.2	Evaluation methods and activities
5.3	Skills required when evaluating specific security assurance classes
5.3.1	General
5.3.2	ADV (Development) Class
5.3.3	AGD (Guidance Documents) Class
5.3.4	ALC (Life-Cycle Support) Class
5.3.5	ASE and APE (ST and PP evaluation) Classes
5.3.6	ATE (Tests) Class
5.3.7	AVA (Vulnerability Assessment) Class
5.3.8	ACO (Composition) Class
5.4	Skills required when evaluating specific security functional requirement classes
5.4.1	General
5.4.2	Skills required when evaluating the FCS (Cryptographic support) Class
5.5	Skills needed when evaluating specific technologies
6	Experience

7 Education

8 Effectiveness

- 8.1 General**
- 8.2 Effectiveness of the evaluation**
- 8.3 Evaluation scheme responsibilities for evaluator effectiveness**
- 8.4 Effectiveness in performing timely evaluations**
- 8.5 Effectiveness in performing accurate evaluations**
- 8.6 Effectiveness in reporting results**

Annex A (informative) Technology types: Knowledge and skills

- A.1 Knowledge related to specific technology types**
 - A.1.1 General**
 - A.1.2 Access control devices and systems**
 - A.1.3 Biometric systems and devices**
 - A.1.4 Data protection**
 - A.1.5 Databases**
 - A.1.6 Detection devices and systems**
 - A.1.7 ICs, smart-cards and smart-card related devices and systems**
 - A.1.8 Hardware devices**
 - A.1.9 Key management systems**
 - A.1.10 Mobile devices and systems**
 - A.1.11 Multi-function devices**
 - A.1.12 Network and network-related devices and systems**
 - A.1.13 Operating systems**
 - A.1.14 Products for digital signatures**
 - A.1.15 Trusted computing**
- A.2 Skills related to specific technology types**
 - A.2.1 General**
 - A.2.2 Access control devices and systems**
 - A.2.3 Biometric systems and devices**
 - A.2.4 Data protection**
 - A.2.5 Databases**
 - A.2.6 Detection devices and systems**
 - A.2.7 ICs, smart cards and smart card-related devices and systems**
 - A.2.8 Hardware devices**
 - A.2.9 Key Management systems**
 - A.2.10 Mobile devices and systems**
 - A.2.11 Multi-function devices**
 - A.2.12 Network and network-related devices and systems**
 - A.2.13 Operating systems**
 - A.2.14 Products for digital signatures**
 - A.2.15 Trusted computing**

Annex B (informative) Examples of knowledge required for evaluating security assurance requirement classes

- B.1 Knowledge required for specific assurance classes**
 - B.1.1 ADV (Development) Class**
 - B.1.2 AGD (Guidance Documents) Class**
 - B.1.3 ALC (Life-Cycle Support) Class**
 - B.1.4 ASE & APE (ST and PP evaluation) Classes**
 - B.1.5 ATE (Tests) Class**
 - B.1.6 AVA (Vulnerability Assessment) Class**
 - B.1.7 ACO (Composition) Class**

Annex C (informative) Examples of knowledge required for evaluating security functional requirement classes

- C.1 General**
- C.2 Knowledge required for specific security functional requirement classes**
 - C.2.1 FAU (Security Audit) Class**
 - C.2.2 FCO (Communication) Class**
 - C.2.3 FCS (Cryptographic Support) Class**
 - C.2.4 FDP (User Data Protection) Class**

C.2.5	FIA (Identification and Authentication) Class
C.2.6	FMT (Security Management) Class
C.2.7	FPR (Privacy) Class
C.2.8	FPT (Protection of the TSF) Class
C.2.9	FRU (Resource Utilisation) Class
C.2.10	FTA (TOE Access) Class
C.2.11	FTP (Trusted Path/Channels) Class

Page count: 33