

DIN EN ISO/IEC 19896-3:2026-10 (D)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre -
Anforderungen an die Kompetenz des Personals von Konformitätsbewertungsstellen
für IT-Sicherheit - Teil 3: Anforderungen an das Wissen und die Fertigkeiten von
Evaluatoren und Überprüfern nach ISO/IEC 15408 und ISO/IEC 18045 (ISO/IEC 19896-
3:2025); Deutsche Fassung EN ISO/IEC 19896-3:2025

Inhalt	Seite
Europäisches Vorwort	8
Vorwort	9
Einleitung	11
1 Anwendungsbereich	13
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen	13
3.1 Begriffe	14
3.2 Abkürzungen	14
4 Wissen	14
4.1 Erforderliches Wissen für Evaluatoren	14
4.1.1 Allgemeines	14
4.1.2 Wissen um die Normenreihe ISO/IEC 15408 und ISO/IEC 18045	15
4.1.3 Wissen über das Vertrauenswürdigkeitsparadigma	17
4.1.4 Wissen über Informationssicherheit	19
4.1.5 Wissen über die Technologie	19
4.2 Erforderliches Wissen für fachliche Prüfer	21
4.2.1 Allgemeines	21
4.2.2 Wissen um die Normenreihe ISO/IEC 15408 und ISO/IEC 18045	22
4.2.3 Wissen über das Vertrauenswürdigkeitsparadigma	24
4.2.4 Wissen über Informationssicherheit	26
4.2.5 Wissen über die Technologie	27
5 Fertigkeiten	29
5.1 Erforderliche Fertigkeiten für Evaluatoren	29
5.1.1 Allgemeines	29
5.1.2 Grundlegende Evaluierungsfertigkeiten	29
5.1.3 Kernkompetenzen bei der Evaluierung hinsichtlich ISO/IEC 15408-3 und ISO/IEC 18045	30
5.1.4 Erforderliche Fertigkeiten für spezifische Vertrauenswürdigkeitsklassen	31
5.1.5 Erforderliche Fertigkeiten für bestimmte Klassen funktionaler Sicherheitsanforderungen	32
5.1.6 Erforderliche Fertigkeiten für eine bestimmte Technologie	32
5.2 Erforderliche Fertigkeiten für fachliche Prüfer	32
5.2.1 Grundlegende Überprüfungsfertigkeiten	32
5.2.2 Kernkompetenzen bei der Überprüfung hinsichtlich ISO/IEC 15408-3 und ISO/IEC 18045	33
5.2.3 Erforderliche Fertigkeiten für spezifische Vertrauenswürdigkeitsklassen	33
5.2.4 Erforderliche Fertigkeiten für bestimmte Klassen funktionaler Sicherheitsanforderungen	34
5.2.5 Erforderliche Fertigkeiten für eine bestimmte Technologie	34
Anhang A (informativ) Technologietypen: Wissen und Fertigkeiten	35
A.1 Wissen in Bezug auf bestimmte Technologietypen	35

A.1.1	Allgemeines.....	35
A.1.2	Zugangskontrollgeräte und -systeme.....	35
A.1.3	Biometrische Systeme und Geräte.....	36
A.1.4	Datenschutz.....	36
A.1.5	Datenbanken	36
A.1.6	Erkennungsgeräte und -systeme.....	36
A.1.7	ICs, Chipkarten sowie chipkartenbezogene Geräte und Systeme.....	36
A.1.8	Hardwaregeräte.....	37
A.1.9	Schlüsselverwaltungssysteme	37
A.1.10	Mobilgeräte und -systeme	37
A.1.11	Multifunktionsgeräte	38
A.1.12	Netz- und netzbezogene Geräte und Systeme	38
A.1.13	Betriebssysteme	38
A.1.14	Produkte für digitale Signaturen	38
A.1.15	Vertrauenswürdige Datenverarbeitung (Trusted Computing).....	39
A.2	Fertigkeiten in Bezug auf bestimmte Technologietypen.....	39
A.2.1	Allgemeines.....	39
A.2.2	Zugangskontrollgeräte und -systeme.....	39
A.2.3	Biometrische Systeme und Geräte.....	40
A.2.4	Datenschutz.....	40
A.2.5	Datenbanken	40
A.2.6	Erkennungsgeräte und -systeme.....	40
A.2.7	ICs, Chipkarten sowie chipkartenbezogene Geräte und Systeme.....	40
A.2.8	Hardwaregeräte.....	40
A.2.9	Schlüsselverwaltungssysteme	41
A.2.10	Mobilgeräte und -systeme	41
A.2.11	Multifunktionsgeräte	41
A.2.12	Netz- und netzbezogene Geräte und Systeme	41
A.2.13	Betriebssysteme	41
A.2.14	Produkte für digitale Signaturen	41
A.2.15	Vertrauenswürdige Datenverarbeitung (Trusted Computing).....	41
A.3	Mögliche Ansätze und Verfahren für die Entwicklung von Wissen und Fertigkeiten.....	41
Anhang B (informativ) Beispiele für Wissen und Fertigkeiten, die für die Evaluierung von		
	Klassen der Vertrauenswürdigkeitsanforderung erforderlich sind	43
B.1	Allgemeines.....	43
B.2	Erforderliches Wissen für bestimmte Vertrauenswürdigkeitsklassen.....	43
B.2.1	ADV-Klasse (Entwicklung)	43
B.2.2	AGD-Klasse (Leitfäden)	47
B.2.3	ALC-Klasse (Unterstützung des Lebenszyklus)	47
B.2.4	ASE- und APE-Klassen (ST- und PP-Evaluierung)	51
B.2.5	ATE-Klasse (Prüfungen).....	54
B.2.6	AVA-Klasse (Schwachstellenbewertung).....	56
B.2.7	ACO-Klasse (Zusammensetzung)	58
B.2.8	ACE-Klasse (Evaluierung der Schutzprofilkonfiguration)	59
Anhang C (informativ) Beispiele für Wissen, das für die Evaluierung von Klassen der		
	funktionalen Sicherheitsanforderung erforderlich ist	60
C.1	Allgemeines.....	60
C.2	Erforderliches Wissen für bestimmte Klassen funktionaler Sicherheitsanforderungen	60
C.2.1	FAU-Klasse (Sicherheitsaudit)	60
C.2.2	FCO-Klasse (Kommunikation)	60
C.2.3	FCS-Klasse (kryptographische Unterstützung)	60
C.2.4	FDP-Klasse (Schutz der Benutzerdaten).....	61
C.2.5	FIA-Klasse (Identifizierung und Authentifizierung)	61
C.2.6	FMT-Klasse (Sicherheitsmanagement)	62
C.2.7	FPR-Klasse (Datenschutz)	62
C.2.8	FPT-Klasse (Schutz der TSF).....	62
C.2.9	FRU-Klasse (Nutzung von Ressourcen)	63

C.2.10 FTA-Klasse (TOE-Zugang).....	63
C.2.11 FTP-Klasse (vertrauenswürdiger Pfad/vertrauenswürdige Kanäle)	63
Literaturhinweise	64

Tabellen

Tabelle B.1 — Beispiele für Wissen und Fertigkeiten, die für Evaluatoren der ADV-Klasse erforderlich sind	43
Tabelle B.2 — Beispiele für Wissen und Fertigkeiten, die für Evaluatoren der AGD-Klasse erforderlich sind	47
Tabelle B.3 — Beispiele für Wissen und Fertigkeiten, die für Evaluatoren der ALC-Klasse erforderlich sind	48
Tabelle B.4 — Beispiele für Wissen und Fertigkeiten, die für Evaluatoren der ASE- und der APE-Klasse erforderlich sind	52
Tabelle B.5 — Erforderliches Wissen und erforderliche Fertigkeiten für Evaluatoren der ATE-Klasse.....	54
Tabelle B.6 — Beispiele für Wissen und Fertigkeiten, die für Evaluatoren der AVA-Klasse erforderlich sind	56
Tabelle B.7 — Beispiele für Wissen und Fertigkeiten, die für Evaluatoren der ACO-Klasse erforderlich sind	58