DIN EN ISO/IEC 19896-3

DIN

ICS 35.030 Einsprüche bis 2022-11-23

Entwurf

IT-Sicherheitstechniken – Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit – Teil 3: Anforderungen an die Kenntnisse, Fähigkeiten und Effektivität von Evaluatoren nach ISO/IEC 15408 (ISO/IEC 19896-3:2018); Deutsche und Englische Fassung prEN ISO/IEC 19896-3:2022

IT security techniques –
Competence requirements for information security testers and evaluators –
Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators (ISO/IEC 19896-3:2018);
German and English version prEN ISO/IEC 19896-3:2022

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 (ISO/IEC 19896-3:2018);
Version allemande et anglaise prEN ISO/IEC 19896-3:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-09-23 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

— vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;

— oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;

— oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 87 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Nationales Vorwort

Der Text von ISO/IEC 19896-3:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 19896-3:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitskreis NA 043-04-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 15408 (alle Teile)	siehe	DIN EN ISO/IEC 15408 (alle Teile)
ISO/IEC 17025	siehe	DIN EN ISO/IEC 17025
ISO/IEC 18045	siehe	DIN EN ISO/IEC 18045
ISO/IEC 19896-1	siehe	E DIN EN ISO/IEC 19896-1
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 29101	siehe	DIN EN ISO/IEC 29101
ISO/TS 17574	siehe	DIN CEN ISO/TS17574

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN CEN ISO/TS17574, *Elektronische Gebührenerhebung — Leitfaden für Sicherheitsprofile*

DIN EN ISO/IEC 15408 (alle Teile), *Informationstechnik —IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit*

DIN EN ISO/IEC 17025, *Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien*

DIN EN ISO/IEC 18045, *Informationstechnik — Sicherheitstechniken — Methodik für die Bewertung der IT-Sicherheit*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

DIN EN ISO/IEC 29101, *Informationstechnik — Sicherheitstechniken — Architekturrahmenwerk für Datenschutz*

E DIN EN ISO/IEC 19896-1, *IT-Sicherheitstechniken — Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit —Teil 1: Einführung, Konzepte und allgemeine Anforderungen*

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

– Entwurf –

September 2022

prEN ISO/IEC 19896-3

IT-Sicherheitstechniken – Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit – Teil 3: Anforderungen an die Kenntnisse, Fähigkeiten und Effektivität von Evaluatoren nach ISO/IEC 15408 (ISO/IEC 19896-3:2018)

IT security techniques – Competence requirements for information security testers and evaluators – Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators (ISO/IEC 19896-3:2018)

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 (ISO/IEC 19896-3:2018)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Inhalt

Seite

Europäisches Vorwort . . . 5
Vorwort . . . 6
Einleitung . . . 7
1 Anwendungsbereich . . . 9
2 Normative Verweisungen . . . 9
3 Begriffe . . . 9
4 Wissen . . . 9
4.1 Allgemeines . . . 9
4.2 Wissen um ISO/IEC 15408 und ISO/IEC 18045 . . . 9
4.2.1 ISO/IEC 15408-1 . . . 9
4.2.2 ISO/IEC 15408-2 . . . 10
4.2.3 ISO/IEC 15408-3 . . . 10
4.2.4 ISO/IEC 18045 . . . 11
4.3 Wissen über das Vertrauenswürdigkeitsparadigma . . . 11
4.3.1 Wissen über die Evaluierungsinstanz . . . 11
4.3.2 Wissen über das Evaluierungsprogramm . . . 11
4.3.3 Wissen über das Labor und sein Managementsystem . . . 12
4.4 Wissen über Informationssicherheit . . . 12
4.5 Wissen über die zu evaluierende Technologie . . . 13
4.5.1 Wissen über die zu evaluierende Technologie . . . 13
4.5.2 Schutzprofile, Pakete und unterstützende Dokumente . . . 13
4.6 Erforderliches Wissen für bestimmte Vertrauenswürdigkeitsklassen . . . 13
4.7 Erforderliches Wissen für die Evaluierung spezifischer funktionaler Sicherheitsanforderungen . . . 14
4.8 Notwendiges Wissen für die Evaluierung spezifischer Technologien . . . 14
5 Fertigkeiten . . . 14
5.1 Grundlegende Evaluierungsfertigkeiten . . . 14
5.1.1 Evaluierungsverfahren . . . 14
5.1.2 Evaluierungsinstrumente . . . 14
5.2 Kernkompetenzen bei der Evaluierung nach ISO/IEC 15408-3 und ISO/IEC 18045 . . . 15
5.2.1 Evaluierungsgrundsätze . . . 15
5.2.2 Evaluierungsverfahren und Tätigkeiten . . . 15
5.3 Erforderliche Fertigkeiten bei der Evaluierung spezifischer Vertrauenswürdigkeitsklassen . . . 16
5.3.1 Allgemeines . . . 16
5.3.2 ADV-Klasse (Entwicklung) . . . 16
5.3.3 AGD-Klasse (Leitfäden) . . . 17
5.3.4 ALC-Klasse (Unterstützung des Lebenszyklus) . . . 18
5.3.5 ASE- und APE-Klassen (ST- und PP-Evaluierung) . . . 19
5.3.6 ATE-Klasse (Prüfungen) . . . 19
5.3.7 AVA-Klasse (Schwachstellenbewertung) . . . 20
5.3.8 ACO-Klasse (Zusammensetzung) . . . 21
5.4 Erforderliche Fertigkeiten bei der Evaluierung spezifischer Klassen funktionaler Sicherheitsanforderungen . . . 22
5.4.1 Allgemeines . . . 22
5.4.2 Erforderliche Fertigkeiten bei der Evaluierung der FCS-Klasse (Kryptographische Unterstützung) . . . 22
5.5 Notwendige Fertigkeit bei der Evaluierung spezifischer Technologien . . . 22
6 Erfahrung . . . 23
7 Ausbildung . . . 23
8 Effektivität . . . 24

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

8.1 Allgemeines . . . 24
8.2 Effektivität der Evaluierung . . . 24
8.3 Verantwortlichkeiten im Rahmen des Evaluierungsprogramms für die Effektivität der Evaluatoren . . . 24
8.4 Effektivität bei der Durchführung zeitnaher Evaluierungen . . . 24
8.5 Effektivität bei der Durchführung genauer Evaluierungen . . . 24
8.6 Effektivität bei der Ergebnismeldung . . . 24
Anhang A (informativ) Technologietypen: Wissen und Fertigkeiten . . . 25
A.1 Wissen in Bezug auf bestimmte Technologietypen . . . 25
A.1.1 Allgemeines . . . 25
A.1.2 Zugangskontrollgeräte und -systeme . . . 25
A.1.3 Biometrische Systeme und Geräte . . . 25
A.1.4 Datenschutz . . . 25
A.1.5 Datenbanken . . . 25
A.1.6 Erkennungsgeräte und -systeme . . . 26
A.1.7 ICs, Chipkarten sowie chipkartenbezogene Geräte und Systeme . . . 26
A.1.8 Hardwaregeräte . . . 26
A.1.9 Schlüsselverwaltungssysteme . . . 26
A.1.10 Mobilgeräte und -systeme . . . 26
A.1.11 Multifunktionsgeräte . . . 27
A.1.12 Netz und netzbezogene Geräte und Systeme . . . 27
A.1.13 Betriebssysteme . . . 27
A.1.14 Produkte für digitale Signaturen . . . 27
A.1.15 Vertrauenswürdige Datenverarbeitung (Trusted Computing) . . . 27
A.2 Fertigkeiten in Bezug auf bestimmte Technologietypen . . . 28
A.2.1 Allgemeines . . . 28
A.2.2 Zugangskontrollgeräte und -systeme . . . 28
A.2.3 Biometrische Systeme und Geräte . . . 28
A.2.4 Datenschutz . . . 28
A.2.5 Datenbanken . . . 28
A.2.6 Erkennungsgeräte und -systeme . . . 28
A.2.7 ICs, Chipkarten sowie chipkartenbezogene Geräte und Systeme . . . 28
A.2.8 Hardwaregeräte . . . 29
A.2.9 Schlüsselverwaltungssysteme . . . 29
A.2.10 Mobilgeräte und -systeme . . . 29
A.2.11 Multifunktionsgeräte . . . 29
A.2.12 Netz- und netzbezogene Geräte und Systeme . . . 29
A.2.13 Betriebssysteme . . . 29
A.2.14 Produkte für digitale Signaturen . . . 29
A.2.15 Vertrauenswürdige Datenverarbeitung (Trusted Computing) . . . 29
Anhang B (informativ) Beispiele für Wissen, das für die Evaluierung von Klassen der Vertrauenswürdigkeitsanforderung erforderlich ist . . . 30
B.1 Erforderliches Wissen für bestimmte Vertrauenswürdigkeitsklassen . . . 30
B.1.1 ADV-Klasse (Entwicklung) . . . 30
B.1.2 AGD-Klasse (Leitfäden) . . . 31
B.1.3 ALC-Klasse (Unterstützung des Lebenszyklus) . . . 32
B.1.4 ASE- und APE-Klassen (ST- und PP-Evaluierung) . . . 34
B.1.5 ATE-Klasse (Prüfungen) . . . 34
B.1.6 AVA-Klasse (Schwachstellenbewertung) . . . 35
B.1.7 ACO-Klasse (Zusammensetzung) . . . 36
Anhang C (informativ) Beispiele für Wissen, das für die Evaluierung von Klassen der funktionalen Sicherheitsanforderung erforderlich ist . . . 38
C.1 Allgemeines . . . 38
C.2 Erforderliches Wissen für bestimmte Klassen funktionaler Sicherheitsanforderungen . . . 38
C.2.1 FAU-Klasse (Sicherheitsaudit) . . . 38
C.2.2 FCO-Klasse (Kommunikation) . . . 38
C.2.3 FCS-Klasse (Kryptographische Unterstützung) . . . 38

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

C.2.4 FDP-Klasse (Schutz der Benutzerdaten) 39
C.2.5 FIA-Klasse (Identifizierung und Authentifizierung) 39
C.2.6 FMT-Klasse (Sicherheitsmanagement) 40
C.2.7 FPR-Klasse (Datenschutz) 40
C.2.8 FPT-Klasse (Schutz der TSF) 40
C.2.9 FRU-Klasse (Nutzung von Ressourcen) 40
C.2.10 FTA-Klasse (TOE-Zugang) 41
C.2.11 FTP-Klasse (Vertrauenswürdiger Pfad/Kanäle) 41
Literaturhinweise 42

Tabellen

Tabelle 1 — Erforderliche Fertigkeiten für Evaluatoren der ADV-Klasse 16
Tabelle 2 — Erforderliche Fertigkeiten für Evaluatoren der AGD-Klasse 17
Tabelle 3 — Erforderliche Fertigkeiten für Evaluatoren der ALC-Klasse 18
Tabelle 4 — Erforderliche Fertigkeiten für Evaluatoren der ASE- und APE-Klasse 19
Tabelle 5 — Erforderliche Fertigkeiten für Evaluatoren der ATE-Klasse 19
Tabelle 6 — Erforderliche Fertigkeiten für Evaluatoren der AVA-Klasse 21
Tabelle 7 — Erforderliche Fertigkeiten für Evaluatoren der ACO-Klasse 21
Tabelle B.1 — Erforderliches Wissen für Evaluatoren der ADV-Klasse 30
Tabelle B.2 — Erforderliches Wissen für Evaluatoren der AGD-Klasse 32
Tabelle B.3 — Erforderliches Wissen für Evaluatoren der ALC-Klasse 32
Tabelle B.4 — Erforderliches Wissen für Evaluatoren der ASE- und APE-Klasse 34
Tabelle B.5 — Erforderliches Wissen für Evaluatoren der ATE-Klasse 35
Tabelle B.6 — Erforderliches Wissen für Evaluatoren der AVA-Klasse 36
Tabelle B.7 — Erforderliches Wissen für Evaluatoren der ACO-Klasse 36

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Europäisches Vorwort

Der Text von ISO/IEC 19896-3:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 19896-3:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 19896-3:2018 wurde von CEN als prEN ISO/IEC 19896-3:2022 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques,* erarbeitet.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 19896 kann auf der ISO-Internetseite abgerufen werden.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Einleitung

Die Normenreihe ISO/IEC 15408 ermöglicht die Vergleichbarkeit der Ergebnisse unabhängiger Sicherheitsevaluierungen. Zu diesem Zweck werden gemeinsame Anforderungen an die Sicherheitsfunktionalität von IT-Produkten und an die Vertrauenswürdigkeitsmaßnahmen, die bei einer Sicherheitsevaluierung auf diese IT-Produkte angewendet werden, festgelegt. Viele Zertifizierungs- und Evaluierungsprogramme sowie Evaluierungsinstanzen wurden auf der Grundlage der Normenreihe ISO/IEC 15408 und ISO/IEC 18045 entwickelt, was die Vergleichbarkeit der Ergebnisse von Evaluierungsprojekten ermöglicht.

Ein wichtiger Faktor bei der Sicherstellung der Vergleichbarkeit der Ergebnisse solcher Evaluierungen ist das Verständnis dafür, dass der Evaluierungsprozess die Festlegung sowohl objektiver als auch subjektiver Vertrauenswürdigkeitsmaßnahmen beinhaltet. Daher ist die Kompetenz der einzelnen Evaluatoren wichtig, wenn die Vergleichbarkeit und Wiederholbarkeit der Evaluierungsergebnisse die Grundlage für die gegenseitige Anerkennung sind.

Die ISO/IEC 17025 enthält allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien. In der ISO/IEC 17025:2017, 5.2.1, heißt es: „*Das Personal, das bestimmte Aufgaben ausführt, muss auf der Grundlage einer angemessenen Ausbildung, Schulung, Erfahrung und/oder nachgewiesener Fertigkeiten qualifiziert sein*“.

Dieses Dokument legt eine Grundlage für die Mindestkompetenz von ISO/IEC 15408-Evaluatoren fest, mit dem Ziel, Konformität in den Anforderungen an die Ausbildung von ISO/IEC 15408-Evaluatoren zu schaffen, die mit IT-Produktevaluierungsprogrammen und -instanzen verbunden sind. Es enthält die speziellen Anforderungen zum Nachweis der Kompetenz von Personen bei der Durchführung der Sicherheitsevaluierungen von IT-Produkten in Übereinstimmung mit ISO/IEC 15408 (alle Teile) und ISO/IEC 18045. ISO/IEC 15408-1 beschreibt das allgemeine Rahmenwerk für Kompetenzen einschließlich der verschiedenen Kompetenzelemente: Wissen, Fertigkeiten, Erfahrung, Ausbildung und Effektivität. Dieses Dokument umfasst Wissen und Fertigkeiten insbesondere in den folgenden Bereichen.

— Informationssicherheit

  Wissen: Grundsätze der Informationssicherheit, Eigenschaften der Informationssicherheit, Bedrohungen und Schwachstellen der Informationssicherheit

  Fertigkeiten: Verständnis der Anforderungen an die Informationssicherheit, Verständnis des Kontextes

— Evaluierung der Informationssicherheit

  Wissen: Wissen um ISO/IEC 15408 (alle Teile) und ISO/IEC 18045, Labormanagementsystem

  Fertigkeiten: Grundlegende Evaluierungsfertigkeiten, Kernfertigkeiten bei der Evaluierung, erforderliche Fertigkeiten bei der Evaluierung bestimmter Vertrauenswürdigkeitsklassen, erforderliche Fertigkeiten bei der Evaluierung bestimmter Klassen von funktionalen Sicherheitsanforderungen

— Architektur der Informationssysteme

  Wissen: Evaluierte Technologie

  Fertigkeiten: Verstehen des Zusammenspiels von Sicherheitskomponenten und Informationen

— Prüfung der Informationssicherheit

  Wissen: Prüfverfahren für die Informationssicherheit, Prüfwerkzeuge für die Informationssicherheit, Lebenszyklus der Produktentwicklung, Prüfarten

  Fertigkeiten: Erstellung und Verwaltung eines Informationssicherheitsprüfplans, Gestaltung von Informationssicherheitsprüfungen, Vorbereitung und Durchführung von Informationssicherheitsprüfungen

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Zur Zielgruppe dieses Dokuments gehören Validierungs- und Zertifizierungsinstanzen, Akkreditierungsstellen für Prüflaboratorien, Evaluierungsprogramme, Laboratorien, Evaluatoren und Organisationen, die professionelle Zertifizierungen anbieten.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

1 Anwendungsbereich

Dieses Dokument enthält die speziellen Anforderungen zum Nachweis der Kompetenz von Personen bei der Durchführung von Sicherheitsevaluierungen von IT-Produkten in Übereinstimmung mit ISO/IEC 15408 (alle Teile) und ISO/IEC 18045.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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 (alle Teile), *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 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 19896-1, ISO/IEC 15408-1, ISO/IEC 17025, ISO/IEC 18045 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter http://www.electropedia.org/

3.1
Evaluierungsprogramm
Organisation, die Richtlinien und ein von einer Evaluierunginstanz festgelegtes Regelwerk umsetzt, das die Evaluierungsumgebung, einschließlich der für die Durchführung von IT-Sicherheitsevaluierungen erforderlichen Kriterien und Methodik, definiert

3.2
subjektives Verfahren
Verfahren auf der Grundlage der Erfahrung und des Verständnisses einer bestimmten Person

4 Wissen

4.1 Allgemeines

Wissen ist das, was ein Evaluator weiß und beschreiben kann. Die Unterabschnitte 4.2 bis 4.8 befassen sich mit dem Wissen, das für die Evaluierung nach ISO/IEC 15408 (alle Teile) und ISO/IEC 18045 erforderlich ist.

4.2 Wissen um ISO/IEC 15408 und ISO/IEC 18045

4.2.1 ISO/IEC 15408-1

Alle Evaluatoren müssen über folgendes Wissen verfügen:

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

a) die in ISO/IEC 15408-1 definierten Begriffe;

b) die in ISO/IEC 18045 definierten Begriffe;

c) den Kontext für die Evaluierungen nach ISO/IEC 15408;

d) das allgemeine Modell für die Normenreihe ISO/IEC 15408, das in ISO/IEC 15408-1 beschrieben ist;

e) Anpassung der Sicherheitsanforderungen: Abläufe, Abhängigkeiten zwischen Komponenten und erweiterten Komponenten;

f) Schutzprofile und Pakete;

g) Evaluierung der Ergebnisse; und

h) die Spezifikation von Sicherheitsvorgaben.

4.2.2 ISO/IEC 15408-2

Alle Evaluatoren müssen mit den funktionalen Sicherheitsanforderungen (SFR) der ISO/IEC 15408-2 vertraut sein, die für die Technologietypen verwendet werden, mit denen der Evaluator arbeiten darf, sowie mit allen abhängigen SFR. Die in ISO/IEC 15408-2 angegebenen Klassen von SFR sind:

a) Sicherheitsaudit (FAU);

b) Kommunikation (FCO);

c) kryptographische Unterstützung (FCS);

d) Schutz der Benutzerdaten (FDP);

e) Identifizierungs- und Authentifizierungsrichtlinie (FIA);

f) Sicherheitsmanagement (FMT);

g) Datenschutz (FPR);

h) Schutz der Sicherheitsfunktionen für den Evaluierungsgegenstand (FPT);

i) Nutzung von Ressourcen (FRU);

j) Zugang zum Evaluierungsgegenstand (FTA); und

k) vertrauenswürdiger Pfad/Kanäle (FTP).

4.2.3 ISO/IEC 15408-3

Alle Evaluatoren müssen mit den in ISO/IEC 15408-3 aufgeführten Sicherheitsanforderungen an die Vertrauenswürdigkeit (SAR) vertraut sein, die durch die Sicherheitsvorgaben (ST) festgelegt sind, mit denen der Evaluator berechtigt ist zu arbeiten. Zum Wissen über bestimmte SAR-Komponenten gehören auch diejenigen, an denen der Evaluator berechtigt ist, zu arbeiten. Die in ISO/IEC 15408-3 angegebenen Klassen von SAR sind:

a) Entwicklung (ADV);

b) Leitliniendokumentation (AGD);

c) Unterstützung des Lebenszyklus (ALC);

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

d) Struktur der Sicherheitsvorgabe (ASE);

e) Struktur des Schutzprofils (APE);

f) Prüfungen (ATE);

g) Schwachstellenbewertung (AVA); und

h) Komposition (ACO).

4.2.4 ISO/IEC 18045

Alle Evaluatoren müssen über folgendes Wissen verfügen:

a) der Evaluierungsprozess: dieser Prozess ist in ISO/IEC 18045:2008, Abschnitt 8, beschrieben; und

b) Verfahren und Tätigkeiten der Sicherheitsevaluierung: Diese Informationen sind in ISO/IEC 18045 enthalten.

4.3 Wissen über das Vertrauenswürdigkeitsparadigma

4.3.1 Wissen über die Evaluierungsinstanz

Alle Evaluatoren müssen mit den Anforderungen der Evaluierungsinstanz(en) vertraut sein, die für die Evaluierungsprogramme gelten, für die sie berechtigt sind zu arbeiten.

ANMERKUNG Beispiele für solche Evaluierungsinstanzen umfassen „Common Criteria Recognition Agreement (CCRA)“ und die „Senior Officials Group Information Systems Security (SOG-IS)“.

Die Anforderungen der Evaluierungsinstanzen können u. a. folgende Themen umfassen:

a) den Anwendungsbereich der Evaluierungsinstanz;

b) Anerkennungsvereinbarungen;

c) Richtlinien der Evaluierungsinstanz;

d) Leitlinien für Evaluierungsprogramme, Validierer und Evaluatoren;

e) Interpretationen;

f) unterstützende Dokumente;

g) Wissen über einschlägige Normen; und

h) Qualitätsanforderungen.

4.3.2 Wissen über das Evaluierungsprogramm

Evaluierungsprogramme definieren in der Regel betriebliche Aspekte wie Richtlinien und Verfahren, die für das jeweilige Evaluierungsprogramm spezifisch sind. Solche Punkte basieren oft auf dem Anwendungsbereich des Evaluierungsprogramms.

Alle Evaluatoren müssen über folgendes Wissen verfügen:

a) die Anforderungen des oder der Evaluierungsprogramme, für die sie berechtigt sind zu arbeiten;

BEISPIEL

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

— alle sektorspezifischen Richtlinien, Vorschriften und Gesetze;

— Anforderungen an die Laborgenehmigung für das Evaluierungsprogramm;

— Richtlinien für das Evaluierungsprogramm in Bezug auf Evaluierungsprojekte, einschließlich Aufnahmekriterien, Fristen, Anforderungen an Berichte und Ortsbegehungen;

— Leitlinien für Validierer und Evaluatoren;

— spezifische Interpretationen des Evaluierungsprogramms;

— besondere Leitlinien des Evaluierungsprogramms;

— genehmigte Schutzprofile und die dazugehörigen unterstützenden Dokumente;

— die spezifischen Vertrauenswürdigkeitsverfahren und -tätigkeiten des Evaluierungsprogramms; und

— Anforderungen an die Berichterstattung.

b) die Kompetenzanforderungen des Evaluierungsprogramms für Evaluatoren.

ANMERKUNG Siehe ISO/IEC 18045:2008, A.5, für Leitlinien zu Evaluierungsprogrammen hinsichtlich dieses Themas.

4.3.3 Wissen über das Labor und sein Managementsystem

Alle Evaluatoren müssen über folgendes Wissen verfügen:

a) das Managementsystem des Labors, einschließlich der Richtlinien, Prozesse und Verfahren, die für die Evaluatoren gelten;

b) genehmigte Laborverfahren; und

c) Anforderungen an die Laborkompetenz.

ANMERKUNG Managementsysteme sind sehr unterschiedlich in ihrer Umsetzung. Punkte wie Dokumentenkontrolle, Aufzeichnungskontrolle, Kontrolle nicht konformer Prüf- und/oder Kalibrierungsarbeiten, Umgang mit technischen Aufzeichnungen und Interessenkonflikte liegen jedoch oft in der direkten Verantwortung der Evaluatoren. Die meisten Labormanagementsysteme beruhen auf der ISO/IEC 17025.

4.4 Wissen über Informationssicherheit

Alle Evaluatoren müssen über folgendes Wissen verfügen:

a) Sicherheitsgrundsätze;

b) Sicherheitseigenschaften;

c) Angriffsmechanismen;

d) Konzepte des Angriffspotentials;

e) Lebenszyklen einer sicheren Entwicklung;

f) Sicherheitsprüfung; und

g) Anfälligkeiten und Schwachstellen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

4.5 Wissen über die zu evaluierende Technologie

4.5.1 Wissen über die zu evaluierende Technologie

ISO/IEC 15408 (alle Teile) und ISO/IEC 18045 können für die Evaluierung einer großen Bandbreite von Informationstechnologien verwendet werden. Diese Technologien werden häufig durch Evaluierungsprogramme, Evaluierungsinstanzen oder andere in verschiedene Technologietypen eingeteilt.

Alle Evaluatoren müssen über Wissen zu den von ihnen evaluierten Informationstechnologietypen verfügen, einschließlich der gemeinsamen Sicherheitsarchitekturen, die für diesen Technologietyp eingesetzt werden.

ANMERKUNG Anhang A enthält eine informative Liste von Wissensthemen, die nach häufig identifizierten Technologietypen geordnet sind.

BEISPIEL Zu den häufig identifizierten Technologietypen gehören:

— Zugangskontrollgeräte und -systeme;

— Verschlüsselung, Schlüsselverwaltung und PKI-Systeme, Produkte für digitale Signaturen;

— Datenbanken;

— Betriebssysteme;

— Netz und netzbezogene Geräte und Systeme;

— Mobilgeräte und -systeme;

— Multifunktionsgeräte;

— ICs, Chipkarten sowie chipkartenbezogene Geräte und Systeme;

— Hardwaregeräte;

— Detektionsgeräte und -systeme; und

— Datenschutz, biometrische Systeme und -geräte, vertrauenswürdige Datenverarbeitung.

4.5.2 Schutzprofile, Pakete und unterstützende Dokumente

Alle Evaluatoren müssen über folgendes Wissen verfügen, sofern es auf die von ihnen evaluierte Informationstechnologie anwendbar ist:

a) Schutzprofile, Pakete und alle zugehörigen unterstützenden Dokumente, die im Zusammenhang mit der Arbeit des Evaluators angegeben wurden;

b) das erforderliche Wissen, um zusätzliche Evaluierungsverfahren und Vertrauenswürdigkeitstätigkeiten zu erfüllen, die für eine Evaluierung festgelegt wurde;

c) wie man bestimmt, ob Interpretationen oder Leitlinien zu Schutzprofilen, Paketen und zugehörigen unterstützenden Dokumenten herausgegeben wurden und ob sie auf ein bestimmtes Evaluierungsprojekt anwendbar sind.

4.6 Erforderliches Wissen für bestimmte Vertrauenswürdigkeitsklassen

Die Evaluatoren müssen über das Wissen verfügen, das für die Evaluierungsverfahren und -tätigkeiten erforderlich und für die Vertrauenswürdigkeitsklassen, für die sie berechtigt sind, tätig zu werden, festgelegt ist. Beispiele für das nach ISO/IEC 18045 erforderliche Wissen sind in Anhang B aufgeführt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

4.7 Erforderliches Wissen für die Evaluierung spezifischer funktionaler Sicherheitsanforderungen

Die Evaluatoren müssen über das erforderliche Wissen verfügen, das durch die funktionalen Sicherheitsanforderungen vorgegeben ist, zu deren Evaluierung sie nach ISO/IEC 15408-2 berechtigt sind. Beispiele für das nach ISO/IEC 15408-2 erforderliche Wissen sind in Anhang C aufgeführt.

4.8 Notwendiges Wissen für die Evaluierung spezifischer Technologien

Da die Technologien variieren können und sich ständig weiterentwickeln, ist es nicht möglich, alle erforderlichen Fertigkeiten zu ermitteln. Anhang A enthält eine informative Liste sowohl zum Wissen als auch zu den Fertigkeiten für viele Technologien. Darüber hinaus enthalten die Literaturhinweise zahlreiche technologiebezogene Verweisungen.

Technologiebezogenes Wissen kann durch Erfahrung mit dieser Technologie erworben werden. Eine solche Erfahrung kann durch folgende Maßnahmen erworben werden:

a) Teilnahme an der Ausbildung im Bereich der Technologie;

b) Arbeit als Schulungsteilnehmer an der Seite eines erfahrenen Evaluators;

c) Mitarbeit an der Entwicklung der Technologie; und

d) Erforschung der Technologie.

5 Fertigkeiten

5.1 Grundlegende Evaluierungsfertigkeiten

5.1.1 Evaluierungsverfahren

Alle Evaluatoren müssen über grundlegende Fertigkeiten in Evaluierungsverfahren verfügen. Dazu gehören sowohl objektive als auch subjektive Verfahren, darunter:

a) Probenahme;

b) grundlegende statistische Analyse;

c) Beobachtung;

d) Analyse;

e) Vergleich; und

f) Aufzeichnung von Ergebnissen.

5.1.2 Evaluierungsinstrumente

Der Evaluator muss über die erforderlichen Fertigkeiten verfügen:

a) die Verwendung von Instrumenten, die vom Labor oder dem Evaluierungsprogramm zur Unterstützung der Evaluierung, der Erstellung von Berichten, der Bereitstellung oder des Schutzes von Dokumenten und Ergebnissen festgelegt wurden;

BEISPIEL

— Verschlüsselungstools; und

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

— Dokumentationstools.

b) Spezialtools für bestimmte Evaluierungsaufgaben, wie sie im Labor, im Evaluierungsprogramm oder in den unterstützenden Dokumenten festgelegt sind.

BEISPIEL

— spezielle mathematische Instrumente für die Analyse von Messdaten;

— Tools zur Überprüfung der Implementierung von Kryptoalgorithmen.

5.2 Kernkompetenzen bei der Evaluierung nach ISO/IEC 15408-3 und ISO/IEC 18045

5.2.1 Evaluierungsgrundsätze

Alle Evaluatoren müssen in der Lage sein, ihre Arbeit auf eine Weise auszuführen, die:

a) unparteilich;

b) objektiv;

c) wiederholbar; und

d) reproduzierbar ist.

5.2.2 Evaluierungsverfahren und Tätigkeiten

Alle Evaluatoren müssen über Fertigkeiten in den zentralen Evaluierungsverfahren und -tätigkeiten verfügen, die in ISO/IEC 18045, Schutzprofilen und allen unterstützenden Dokumenten festgelegt sind.

Die folgenden Verben haben in ISO/IEC 18045:2008 eine besondere Bedeutung, und der Evaluator muss in der Ausführung der Tätigkeiten nach den Definitionen in ISO/IEC 18045:2008 erfahren sein. Diese werden durch die folgenden Verben ausgedrückt:

a) prüfen;

b) bestätigen;

c) nachweisen;

d) beschreiben;

e) bestimmen;

f) sicherstellen;

g) erschöpfend sein;

h) untersuchen;

i) erklären;

j) begründen;

k) beweisen;

l) berichten;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

m) aufzeichnen;

n) festlegen;

o) verfolgen; und

p) verifizieren.

ANMERKUNG Diese Begriffe werden entweder in ISO/IEC 15408-1 oder ISO/IEC 18045:2008 definiert und erläutert.

5.3 Erforderliche Fertigkeiten bei der Evaluierung spezifischer Vertrauenswürdigkeitsklassen

5.3.1 Allgemeines

Evaluatoren, die Evaluierungstätigkeiten durchführen, müssen in der Lage sein, Beobachtungsberichte zu verfassen.

Die weiteren erforderlichen Fertigkeiten sind für jede Klasse in Tabelle 1 bis Tabelle 7 aufgeführt. Innerhalb jeder Familie nehmen die erforderlichen Fertigkeiten sowohl in der Tiefe als auch in der Breite zu. Die zusätzlichen Fertigkeiten sind in den höheren Gliedern der Familie aufgeführt, während die größere Tiefe der Fertigkeiten nicht ausdrücklich erwähnt wird, aber bei der Zulassung von Evaluatoren berücksichtigt werden muss.

BEISPIEL 1 Ein Evaluator, der zur Evaluierung von ADV_FSP.2 berechtigt ist, muss in der Lage sein, Suchverknüpfungen der SFR zu überprüfen, bevor er die Genehmigung für ADV_FSP.3 erhält.

BEISPIEL 2 Für ADV_TDS.1 sind nur grundlegende Fertigkeiten bezüglich der TOE-Architektur erforderlich, während für ADV_TDS.6 Fertigkeiten im Umgang mit formalen Verfahren für die Architektur erforderlich sind.

5.3.2 ADV-Klasse (Entwicklung)

Evaluatoren, die Evaluierungstätigkeiten im Zusammenhang mit der ADV-Klasse durchführen, müssen über die in Tabelle 1 aufgeführten Fertigkeiten für die Vertrauenswürdigkeitskomponenten bis einschließlich der von ihnen zu evaluierenden Komponente verfügen.

Tabelle 1 — Erforderliche Fertigkeiten für Evaluatoren der ADV-Klasse

Vertrauens-würdigkeits-komponente	Erforderliche Evaluierungsfertigkeiten
ADV_ARC.1	a) Fähigkeit, architektonische Informationen mit anderen für die Evaluierung bereitgestellten Nachweise abzugleichen.
ADV_FSP.1	a) Fähigkeit, Programm- und Anwendungsschnittstellen zu identifizieren; b) Fähigkeit, die TSFI zu bestimmen.
ADV_FSP.2	Keine zusätzlichen Anforderungen.
ADV_FSP.3	c) Fähigkeit, die Suchverknüpfungen der SFR zu überprüfen;
ADV_FSP.4	Keine zusätzlichen Anforderungen.
ADV_FSP.5	d) Fähigkeit, die halbformale Sprache zu verstehen;
ADV_FSP.6	e) Fähigkeit, die formale Sprache zu verstehen; f) Fähigkeit, die Korrektheit des formalen Modells und die Vollständigkeit der Argumentation zu verifizieren.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Tabelle 1 (*fortgesetzt*)

Vertrauens-würdigkeits-komponente	Erforderliche Evaluierungsfertigkeiten
ADV_IMP.1	a) Verwendung von Probenahmeverfahren; b) Fähigkeit, den Quellcode oder die Hardware-Diagramme und/oder den Code der IC-Hardware-Entwurfssprache oder die bei der Implementierung des TOE verwendeten Entwurfsdaten zu lesen und zu verstehen; c) Fähigkeit zur Verwendung von Tools, die eine Enttarnung oder Entschleierung ermöglichen; d) Fähigkeit, Generierungstools, ihre Verwendung und ihre Auswirkungen zu verstehen. BEISPIEL Konfigurationen des Compilers.
ADV_IMP.2	Keine zusätzlichen Anforderungen.
ADV_INT.1	Keine zusätzlichen Anforderungen.
ADV_INT.2	a) Fähigkeit, die für die TSF relevanten Normen zu ermitteln, um zu bestimmen, ob die TSF gut strukturiert ist;
ADV_INT.3	b) Fähigkeit, die Komplexität der TSF-Interna zu beurteilen;
ADV_SPM.1	a) Fähigkeit, das Modell der Sicherheitsrichtlinie zu verstehen und zu bestimmen, ob es vollständig ist;
ADV_TDS.1	a) Fähigkeit, die Architektur des TOE zu verstehen.
ADV_TDS.2	Keine zusätzlichen Anforderungen.
ADV_TDS.3	Keine zusätzlichen Anforderungen.
ADV_TDS.4	Keine zusätzlichen Anforderungen.
ADV_TDS.5	Keine zusätzlichen Anforderungen.
ADV_TDS.6	Keine zusätzlichen Anforderungen.

5.3.3 AGD-Klasse (Leitfäden)

Evaluatoren, die Evaluierungstätigkeiten im Zusammenhang mit der AGD-Klasse durchführen, müssen über die in Tabelle 2 aufgeführten Fertigkeiten für die von ihnen zu evaluierenden Vertrauenswürdigkeitskomponenten verfügen.

Tabelle 2 — Erforderliche Fertigkeiten für Evaluatoren der AGD-Klasse

Vertrauens-würdigkeits-komponente	Erforderliche Evaluierungsfertigkeiten
AGD.OPE.1	a) Fähigkeit, die Korrektheit und Sicherheit des Vorgangs anhand von Nachweisen zu verstehen;
AGD_PRE.1	a) Fähigkeit, die Korrektheit und Sicherheit der Installation anhand von Nachweisen zu verstehen;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

5.3.4 ALC-Klasse (Unterstützung des Lebenszyklus)

Evaluatoren, die Evaluierungstätigkeiten im Zusammenhang mit der ALC-Klasse durchführen, müssen über die in Tabelle 3 aufgeführten Fertigkeiten für die von ihnen zu evaluierenden Vertrauenswürdigkeitskomponenten verfügen.

Tabelle 3 — Erforderliche Fertigkeiten für Evaluatoren der ALC-Klasse

Vertrauens-würdigkeits-komponente	Erforderliche Evaluierungsfertigkeiten
ALC_CMC.1	a) Fähigkeit, die Anwendung des CM-Systems wie im CM-Plan beschrieben zu beobachten;
ALC_CMC.2	Keine zusätzlichen Anforderungen.
ALC_CMC.3	Keine zusätzlichen Anforderungen.
ALC_CMC.4	Keine zusätzlichen Anforderungen.
ALC_CMC.5	Keine zusätzlichen Anforderungen.
ALC_CMS.1	a) Fähigkeit, das Versions- und Identifikationsschema zu verstehen; b) Fähigkeit, zu bestimmen, ob Konfigurationselemente eindeutig identifiziert sind.
ALC_CMS.2	Keine zusätzlichen Anforderungen.
ALC_CMS.3	Keine zusätzlichen Anforderungen.
ALC_CMS.4	Keine zusätzlichen Anforderungen.
ALC_CMS.5	Keine zusätzlichen Anforderungen.
ALC_DEL.1	a) Fähigkeit, schriftliche Liefer- und Installationsverfahren zu befolgen.
ALC_DVS.1	a) Planung der Ortsbegehung; b) Techniken zur Standort- und Personalbeurteilung; c) Fähigkeit, die Anwendung von Sicherheitsmaßnahmen während der Entwicklung und Wartung des TOE, wie sie in der Sicherheitsdokumentation der Entwicklung beschrieben sind, zu beobachten; d) Fähigkeit, die praktische Anwendung der in den Lieferunterlagen beschriebenen Lieferverfahren zu beobachten.
ALC_DVS.2	Keine zusätzlichen Anforderungen.
ALC_FLR.1	a) Fähigkeit, Prozesse zur Behebung von Fehlern zu verstehen.
ALC_FLR.2	Keine zusätzlichen Anforderungen.
ALC_LCD.1	a) Fähigkeit, die vom Entwickler dargelegten Lebenszyklusprozesse zu analysieren.
ALC_LCD.2	Keine zusätzlichen Anforderungen.
ALC_TAT.1	a) Fähigkeit, die vom Entwickler dargelegten Tools und Techniken zu analysieren.
ALC_TAT.2	Keine zusätzlichen Anforderungen.
ALC_TAT.3	Keine zusätzlichen Anforderungen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

5.3.5 ASE- und APE-Klassen (ST- und PP-Evaluierung)

Evaluatoren, die Evaluierungstätigkeiten im Zusammenhang mit der ASE-Klasse durchführen, müssen über die in Tabelle 4 aufgeführten Fertigkeiten für die von ihnen zu evaluierenden Vertrauenswürdigkeitskomponenten verfügen.

Tabelle 4 — Erforderliche Fertigkeiten für Evaluatoren der ASE- und APE-Klasse

Vertrauenswürdigkeits-komponente		Erforderliche Fertigkeiten des Evaluators
ASE_CCL.1	APE_CCL.1	a) Fähigkeit, die Richtigkeit des Konformitätsanspruchs zu überprüfen.
ASE_ECD.1	APE_ECD.1	a) Fähigkeit zu verstehen, dass die Definition der erweiterten Komponenten korrekt ist.
ASE_INT.1	APE_INT.1	a) Fähigkeit zu verstehen, dass die Einleitung den TOE und den Kontext des TOE korrekt beschreibt.
ASE_OBJ.1	APE_OBJ.1	a) Fähigkeit festzustellen, ob die Sicherheitszielsetzungen die Definition des Sicherheitsproblems adäquat und vollständig erfüllen; b) Fähigkeit festzustellen, ob die Sicherheitszielsetzungen korrekt zwischen den Sicherheitszielsetzungen des TOE und den Sicherheitszielsetzungen für die TOE-Umgebung aufgeteilt sind und ob sie zusammen die Definition des Sicherheitsproblems erfüllen.
ASE_OBJ.2	APE_OBJ.2	Keine zusätzlichen Anforderungen.
ASE_REQ.1	APE_REQ.1	a) Fähigkeit festzustellen, dass die Sicherheitsanforderungen klar, eindeutig und genau definiert sind.
ASE_REQ.2	APE_REQ.2	Keine zusätzlichen Anforderungen.
ASE_SPD.1	APE_SPD.1	a) Fähigkeit zu verstehen, dass die Definition des Sicherheitsproblems korrekt ist.
ASE_TSS.1		a) Fähigkeit zur Zuordnung des Narrativs zu bestimmten SFR.

5.3.6 ATE-Klasse (Prüfungen)

Evaluatoren, die Evaluierungstätigkeiten im Zusammenhang mit der ATE-Klasse durchführen, müssen über die in Tabelle 5 aufgeführten Fertigkeiten für die von ihnen zu evaluierenden Vertrauenswürdigkeitskomponenten verfügen.

Tabelle 5 — Erforderliche Fertigkeiten für Evaluatoren der ATE-Klasse

Vertrauens-würdigkeits-komponente	Erforderliche Fertigkeiten des Evaluators
ATE_COV.1	a) Fähigkeit, die dargestellte Prüfabdeckung zu verstehen; b) Fähigkeit, Prüfungen zu verstehen und zu verifizieren, dass die Ergebnisse der Prüfungen korrekt sind;
ATE_COV.2	Keine zusätzlichen Anforderungen.
ATE_COV.3	Keine zusätzlichen Anforderungen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Tabelle 5 (*fortgesetzt*)

Vertrauens-würdigkeits-komponente	Erforderliche Fertigkeiten des Evaluators
ATE_DPT.1	a) Fähigkeit, die vom Entwickler bereitgestellte Dokumentation zur Prüfabdeckung zu verstehen; b) Fähigkeit, das Prüfen auf der Ebene von Teilsystemen zu verstehen.
ATE_DPT.2	a) Fähigkeit, das Prüfen auf Modulebene zu verstehen.
ATE_DPT.3	Keine zusätzlichen Anforderungen.
ATE_DPT.4	Keine zusätzlichen Anforderungen.
ATE_FUN.1	a) Fähigkeit, die vom Entwickler bereitgestellte Dokumentation zur Funktionsprüfung zu verstehen.
ATE_FUN.2	Keine zusätzlichen Anforderungen.
ATE_IND.1	a) Entwicklung eines Prüfplans; b) Entwicklung geeigneter Prüffälle; c) Konfiguration des TOE; d) Aufbau und Konfiguration der TOE-Umgebung; e) Aufrechterhaltung der Integrität der Prüfumgebung; f) Konfigurieren und Verwenden der im Prüfplan angegebenen Prüfwerkzeuge; g) Inbetriebnahme geeigneter Test-Harnische und Testskripte. ANMERKUNG Dies kann die Verwendung von Programmiersprachen, Skriptsprachen und Debugging-Funktionen umfassen.
ATE_IND.2	Keine zusätzlichen Anforderungen.
ATE_IND.3	Keine zusätzlichen Anforderungen.

5.3.7 AVA-Klasse (Schwachstellenbewertung)

Evaluatoren, die Evaluierungstätigkeiten im Zusammenhang mit der AVA-Klasse durchführen, müssen über die in Tabelle 6 aufgeführten Fertigkeiten für die von ihnen zu evaluierenden Vertrauenswürdigkeitskomponenten verfügen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Tabelle 6 — Erforderliche Fertigkeiten für Evaluatoren der AVA-Klasse

Vertrauens-würdigkeits-komponente	Erforderliche Fertigkeiten des Evaluators
AVA_VAN.1	a) Fähigkeit, geeignete Schlüsselwörter für die Suche nach Schwachstellen zu identifizieren; b) Fähigkeit, geeignete Informationsquellen für öffentlich bekannte Schwachstellen für einen bestimmten TOE zu identifizieren; c) Fähigkeit, den Nachweis der Schwachstellenanalyse zu verstehen und zu verifizieren, dass das Ergebnis des Nachweises korrekt ist; d) Fähigkeit zur Analyse von Ursache-Wirkungs-Beziehungen der TOE-Funktionalität; e) Fähigkeit, Restanfälligkeiten zu identifizieren; f) Fähigkeit, das Angriffspotential zu berechnen.
AVA_VAN.2	Keine zusätzlichen Anforderungen.
AVA_VAN.3	g) Entwicklung der Fehlerhypothese;
AVA_VAN.4	Keine zusätzlichen Anforderungen.
AVA_VAN.5	Keine zusätzlichen Anforderungen.

5.3.8 ACO-Klasse (Zusammensetzung)

Evaluatoren, die Evaluierungstätigkeiten im Zusammenhang mit der ACO-Klasse durchführen, müssen über die in Tabelle 7 aufgeführten Fertigkeiten für die von ihnen zu evaluierenden Vertrauenswürdigkeitskomponenten verfügen.

Tabelle 7 — Erforderliche Fertigkeiten für Evaluatoren der ACO-Klasse

Vertrauens-würdigkeits-komponente	Erforderliche Fertigkeiten des Evaluators
ACO_COR.1	Keine zusätzlichen Anforderungen.
ACO_DEV.1	Keine zusätzlichen Anforderungen.
ACO_DEV.2	Keine zusätzlichen Anforderungen.
ACO_DEV.3	Keine zusätzlichen Anforderungen.
ACO_REL.1	Keine zusätzlichen Anforderungen.
ACO_REL.2	Keine zusätzlichen Anforderungen.
ACO_CTT.1	a) Die für die ADV_FSP-Klasse ermittelten Fertigkeiten sind in Tabelle 1 aufgeführt;
ACO_CTT.2	Keine zusätzlichen Anforderungen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

Tabelle 7 (*fortgesetzt*)

Vertrauens-würdigkeits-komponente	Erforderliche Fertigkeiten des Evaluators
ACO_VUL.1	a) Die für die AVA_VAN-Klasse ermittelten Fertigkeiten sind in Tabelle 6 aufgeführt; b) Fähigkeit zu bestimmen, ob die Annahmen und Ziele, die für jede der Komponenten der Betriebsumgebung festgelegt wurden, auch für einen zusammengesetzten TOE zutreffen; c) Fähigkeit, Schwachstellen zu identifizieren, die durch die Zusammensetzung entstanden sind; d) Fähigkeit, Penetrationstests durchzuführen.
ACO_VUL.2	Keine zusätzlichen Anforderungen.
ACO_VUL.3	Keine zusätzlichen Anforderungen.

5.4 Erforderliche Fertigkeiten bei der Evaluierung spezifischer Klassen funktionaler Sicherheitsanforderungen

5.4.1 Allgemeines

Für jede Klasse muss der Evaluator in der Lage sein:

a) die Einhaltung einschlägiger technologischer Normen zu verstehen und zu prüfen; und

b) nach potentiellen Schwachstellen und Seitenkanälen zu suchen.

5.4.2 Erforderliche Fertigkeiten bei der Evaluierung der FCS-Klasse (Kryptographische Unterstützung)

a) Fähigkeit, zu bestimmen, ob kryptographische Algorithmen und Protokolle korrekt implementiert sind.

5.5 Notwendige Fertigkeit bei der Evaluierung spezifischer Technologien

Da die Technologien variieren können und sich ständig weiterentwickeln, ist es nicht möglich, alle erforderlichen Fertigkeiten zu ermitteln. Anhang A enthält eine Liste sowohl zum Wissen als auch zu den Fertigkeiten für einige Technologien.

Technologiebezogene Fertigkeiten können durch Erfahrung mit dieser Technologie erworben werden. Eine solche Erfahrung kann durch folgende Maßnahmen erworben werden:

a) Teilnahme an technologiebezogenen Schulungen;

b) Arbeit als Schulungsteilnehmer an der Seite eines erfahrenen Evaluators;

c) Mitarbeit an der Entwicklung solcher Technologien; und

d) Erforschung der Technologie.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10

6 Erfahrung

Erfahrungen mit den in Abschnitt 5 genannten Kernkompetenzen der Evaluierung werden während der ersten und nachfolgenden Evaluierungen eines Evaluators gesammelt. Als Praktikant sollte diese Erfahrung unter der Aufsicht und/oder Anleitung eines anderen kompetenten Evaluators gesammelt werden.

Frühere Erfahrungen mit Aufgaben im Zusammenhang mit der Anwendung von ISO/IEC 15408 und den zugehörigen Dokumenten, einschließlich, aber nicht beschränkt auf die Durchführung damit verbundener Arbeiten wie Beratung, Produktentwicklung, Forschung und Spezifikation von Anforderungen, können zu den für die Kompetenz erforderlichen Wissenselementen beitragen.

7 Ausbildung

Alle Evaluatoren sollten über einen Hochschulabschluss verfügen, z. B. einen Associate-, Bachelor- oder höheren Abschluss, der für die in ISO/IEC 15408 behandelten Anforderungen und die Anforderungen an die Evaluierungsmethodik in ISO/IEC 18045 relevant ist.

Alle Evaluatoren müssen mindestens nachweisen, dass sie entweder:

a) einen angemessenen Hochschulabschluss mit einem mindestens 3-jährigen Studium in Disziplinen, die spezifische technische Fachgebiete mit Bezug zur IT oder IT-Sicherheit umfassen; oder

b) über Erfahrungen verfügen, die dem durch ein Hochschulstudium erworbenen Wissen, den Fertigkeiten und der Effektivität in Disziplinen, die mit IT oder IT-Sicherheit zu tun haben, gleichwertig sind.

BEISPIEL Beispiele für spezifische technische Fachrichtungen beinhalten:

— Ingenieurswesen;

— Elektrotechnik;

— Maschinenbau;

— Werkstofftechnik;

— Datenverarbeitungstechnik;

— Technische Informatik;

— Informatik;

— Rechennetze;

— Cybersicherheit;

— Physik;

— formale Mathematik;

— Informationssysteme; und

— Softwareentwicklung und -sicherheit.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-3:2022-10