DIN EN ISO/IEC 19896-3

DIN

ICS 35.030

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 Fassung EN ISO/IEC 19896-3:2023

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 version EN ISO/IEC 19896-3:2023

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 EN ISO/IEC 19896-3:2023

Gesamtumfang 50 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-3:2024-09

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 EN ISO/IEC 19896-3:2023 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).

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	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/TS 17574 (DIN SPEC 91117)

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: DIN EN ISO/IEC 19896-3:2024-09

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN CEN ISO/TS 17574 (DIN SPEC 91117), *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*

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: DIN EN ISO/IEC 19896-3:2024-09

– Leerseite –

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-3:2024-09

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 19896-3

Januar 2023

ICS 35.030

Deutsche Fassung

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)

Diese Europäische Norm wurde vom CEN am 9. Januar 2023 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC-Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-3:2024-09

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 19896-3:2024-09

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: DIN EN ISO/IEC 19896-3:2024-09

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: DIN EN ISO/IEC 19896-3:2024-09

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 EN ISO/IEC 19896-3:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juli 2023 und etwaige entgegenstehende nationale Normen müssen bis Juli 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN-CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 19896-3:2018 wurde von CEN-CENELEC als EN ISO/IEC 19896-3:2023 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-3:2024-09

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: DIN EN ISO/IEC 19896-3:2024-09

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: DIN EN ISO/IEC 19896-3:2024-09

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: DIN EN ISO/IEC 19896-3:2024-09

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:

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-3:2024-09

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 Festlegung von Sicherheitsvorgaben.

4.2.2 ISO/IEC 15408-2

Alle Evaluatoren müssen mit den funktionalen Sicherheitsanforderungen (SFR) von 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 müssen auch diejenigen gehören, 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: DIN EN ISO/IEC 19896-3:2024-09

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 19896-3:2024-09