DIN EN ISO/IEC 19896-1

DIN

ICS 35.030 Einsprüche bis 2022-11-23

Entwurf

IT-Sicherheitstechniken – Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit – Teil 1: Einführung, Konzepte und allgemeine Anforderungen (ISO/IEC 19896-1:2018); Deutsche und Englische Fassung prEN ISO/IEC 19896-1:2022

IT security techniques –
Competence requirements for information security testers and evaluators –
Part 1: Introduction, concepts and general requirements (ISO/IEC 19896-1:2018);
German and English version prEN ISO/IEC 19896-1:2022

Techniques de sécurité IT –
Exigences de compétence pour l'information testeurs d'assurance et les évaluateurs –
Partie 1: Introduction, concepts et exigences générales (ISO/IEC 19896-1:2018);
Version allemande et anglaise prEN ISO/IEC 19896-1:2022

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 35 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

Nationales Vorwort

Der Text von ISO/IEC 19896-1:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 19896-1:2022 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 17000	siehe	DIN EN ISO/IEC 17000
ISO/IEC 17024	siehe	DIN EN ISO/IEC 17024
ISO/IEC 17025	siehe	DIN EN ISO/IEC 17025
ISO/IEC 17065	siehe	DIN EN ISO/IEC 17065
ISO/IEC 18045	siehe	DIN EN ISO/IEC 18045
ISO/IEC 19790	siehe	DIN EN ISO/IEC 19790

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

Nationaler Anhang NA
(informativ)

Literaturhinweise

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

DIN EN ISO/IEC 17000, *Konformitätsbewertung — Begriffe und allgemeine Grundlagen*

DIN EN ISO/IEC 17024, *Konformitätsbewertung — Allgemeine Anforderungen an Stellen, die Personen zertifizieren*

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

DIN EN ISO/IEC 17065, *Konformitätsbewertung — Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren*

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

DIN EN ISO/IEC 19790, *Informationstechnik — Sicherheitstechniken — Sicherheitsanforderungen für kryptografische Module*

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

– Entwurf –

September 2022

prEN ISO/IEC 19896-1

IT-Sicherheitstechniken – Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit – Teil 1: Einführung, Konzepte und allgemeine Anforderungen (ISO/IEC 19896-1:2018)

IT security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements (ISO/IEC 19896-1:2018)

Techniques de sécurité IT – Exigences de compétence pour l'information testeurs d'assurance et les évaluateurs – Partie 1: Introduction, concepts et exigences générales (ISO/IEC 19896-1:2018)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

Inhalt

Seite

Europäisches Vorwort **3**
Vorwort **4**
Einleitung **5**
1 Anwendungsbereich **6**
2 Normative Verweisungen **6**
3 Begriffe **6**
4 Konzepte **7**
5 Kompetenzelemente **8**
5.1 Kompetenzen **8**
5.2 Wissen **8**
5.3 Fertigkeiten **9**
5.4 Erfahrung **10**
5.5 Ausbildung **10**
5.6 Effektivität **10**
6 Kompetenzstufen **10**
6.1 Allgemeines **10**
6.2 Stufe 1 (Associate) **10**
6.3 Stufe 2 (Fachkraft) **11**
6.4 Stufe 3 (Manager) **11**
6.5 Stufe 4 (Chef) **11**
7 Messung der Kompetenzelemente **11**
7.1 Wissen **11**
7.2 Fertigkeiten **11**
7.3 Erfahrung **12**
7.4 Ausbildung **12**
7.5 Effektivität **12**
7.6 Aufzeichnung der Kompetenzelemente **12**
Anhang A (informativ) **Rahmenbedingungen für die Beschreibung von Kompetenzanforderungen** **13**
Anhang B (informativ) **Exemplarische Aufzeichnungen für Erfahrung und Kompetenz** **15**
Literaturhinweise **16**

Tabellen

Tabelle A.1 — Nachweis der Kompetenzanforderungen für Stufe 1 . . . . . **13**
Tabelle A.2 — Nachweis der Kompetenzanforderungen für Stufe 2 . . . . . **13**
Tabelle A.3 — Nachweis der Kompetenzanforderungen für Stufe 3 (Manager) **14**
Tabelle A.4 — Nachweis der Kompetenzanforderungen für Stufe 4 (Chef) **14**
Tabelle B.1 — Beispiel für den Nachweis der Erfahrung **15**
Tabelle B.2 — Beispiel für den Nachweis der Kompetenz **15**

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

Europäisches Vorwort

Der Text von ISO/IEC 19896-1:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 19896-1:2022 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 19896-1:2018 wurde von CEN als prEN ISO/IEC 19896-1:2022 ohne irgendeine Abänderung genehmigt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

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.

Eine Erläuterung zum freiwilligen Charakter von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO) hinsichtlich technischer Handelshemmnisse (TBT) berücksichtigt, enthält der folgende Link: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC 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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

Einleitung

Ziel der Normenreihe ISO/IEC 19896 ist es, die grundlegenden Konzepte im Zusammenhang mit der Kompetenz der Personen bereitzustellen, die für die Durchführung von Sicherheitsevaluierungen und Konformitätsprüfungen von IT-Produkten verantwortlich sind. Die Normenreihe ISO/IEC 19896 bietet das Rahmenwerk und die fachlichen Anforderungen, die die Mindestkompetenz für die Personen, die Sicherheitsevaluierungen von IT-Produkten und Konformitätsprüfungen unter Verwendung bewährter Normen durchführen, festlegen.

Um dieses Ziel zu erreichen, umfasst die Normenreihe ISO/IEC 19896 Folgendes:

a) die Begriffe rund um das Thema Kompetenz bei Evaluatoren und Testern der IT-Produktsicherheit;

b) die grundlegenden Konzepte in Bezug auf die Kompetenz bei Evaluatoren und Testern der IT-Produktsicherheit; und

c) die Mindestanforderungen an die Kompetenz von Evaluatoren und Testern der IT-Produktsicherheit zur Durchführung von IT-Produktprüfungen/-evaluierungen.

Die Normenreihe ISO/IEC 19896 ist von Interesse für:

a) Spezialisten zur Evaluierung der Informationssicherheit und Konformitätsprüfung;

b) Genehmigungsinstanzen für die Evaluierung der Informationssicherheit und Konformitätsprüfung;

c) Laboratorien für die Evaluierung der Informationssicherheit und Konformitätsprüfung;

d) Lieferanten oder Technologieanbieter, deren IT-Produkte Gegenstand von Evaluierungen der Vertrauenswürdigkeit der Informationssicherheit oder Konformitätsprüfungen sein können;

e) Organisationen, die berufliche Zugangsdaten oder Anerkennungen anbieten.

Die Normenreihe ISO/IEC 19896 ist in folgende Teile gegliedert, die sich mit der Kompetenz von Fachkräften im Bereich Evaluierung und Prüfung befassen.

Das vorliegende Dokument enthält in der Einleitung und den Konzepten einen Überblick über die Definitionen, die grundlegenden Konzepte und eine allgemeine Beschreibung des Rahmens, der für die Vermittlung der Kompetenzanforderungen für bestimmte Fachbereiche verwendet wird. Dieses Dokument zielt darauf ab, grundlegendes Wissen bereitzustellen, das notwendig ist, um das in den anderen Teilen der Normenreihe ISO/IEC 19896 vorgestellte Rahmenwerk angemessen zu nutzen.

ISO/IEC 19896-2 beschreibt die Mindestanforderungen an die Kompetenz von Konformitätstestern, die mit ISO/IEC 19790 und den zugehörigen Normen arbeiten, auf jeder Kompetenzstufe.

ISO/IEC 19896-3 beschreibt die Mindestanforderungen an die Kompetenz von Evaluatoren der Informationssicherheit, die mit ISO/IEC 15408 (alle Teile) und den zugehörigen Normen arbeiten, auf jeder Kompetenzstufe.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

1 Anwendungsbereich

Dieses Dokument legt Begriffe fest und bietet eine übersichtliche Zusammenstellung von Konzepten und Beziehungen zum Verständnis der Kompetenzanforderungen an Spezialisten zur Konformitätsprüfung und Evaluierung der Vertrauenswürdigkeit der Informationssicherheit. Damit wird die Grundlage für ein gemeinsames Verständnis der Konzepte und Grundsätze geschaffen, die für die Normenreihe ISO/IEC 19896 in den verschiedenen Benutzergemeinschaften von zentraler Bedeutung sind. Es bietet grundlegende Informationen für Nutzer der Normenreihe ISO/IEC 19896.

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 17000, *Conformity assessment — Vocabulary and general principles*

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 17000, ISO/IEC 17025 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
Kompetenz
Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

[QUELLE: ISO/IEC 17024:2012, 3.6]

3.2
Konformitätstester
Tester
Person, die mit der Durchführung von Prüftätigkeiten nach einer bestimmten Norm für Konformitätsprüfungen und der zugehörigen Prüfmethodik beauftragt ist

Anmerkung 1 zum Begriff: Ein Beispiel für eine solche Norm ist ISO/IEC 19790 und die in ISO/IEC 24759 beschriebene Prüfmethodik.

3.3
Ausbildung
Prozess des Erhalts oder der Bereitstellung eines systematischen Unterrichts, insbesondere an einer Schule oder Universität

3.4
Effektivität
Fähigkeit zur produktiven Anwendung von Wissen und Fertigkeiten, gekennzeichnet durch Verhaltensattribute wie Eignung, Initiative, Begeisterung, Bereitschaft, Kommunikationsstärke, Teamfähigkeit und Führungsqualitäten

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10

3.5
Evaluator
Person, die mit der Durchführung von Evaluierungen nach einer bestimmten Evaluierungsnorm und der zugehörigen Evaluierungsmethodik beauftragt ist

Anmerkung 1 zum Begriff: Ein Beispiel für Evaluierungsnormen ist ISO/IEC 15408 (alle Teile) mit der zugehörigen Evaluierungsmethodik, die in ISO/IEC 18045 beschrieben ist.

3.6
Erfahrung
praktische Beteiligung an Projekten im Zusammenhang mit dem Zuständigkeitsbereich

3.7
Wissen
Fakten, Informationen, Wahrheiten, Grundsätze oder Erkenntnisse, die durch Erfahrung oder Bildung erworben wurden

Anmerkung 1 zum Begriff: Ein Beispiel für Wissen ist die Fähigkeit, die verschiedenen Teile einer Informationsvertrauenswürdigkeitsnorm zu beschreiben.

[QUELLE: ISO/IEC TS 17027:2014, 2.56, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.8
Laboratorium
Organisation mit einem Managementsystem, das Evaluierungs- und/oder Prüfarbeiten in Übereinstimmung mit einer definierten Reihe von Richtlinien und Verfahren und unter Verwendung einer definierten Methodik für die Prüfung oder Evaluierung der Sicherheitsfunktionalität von IT-Produkten durchführt

Anmerkung 1 zum Begriff: Diese Organisationen werden von den verschiedenen Genehmigungsinstanzen oft mit anderen Bezeichnungen versehen. Zum Beispiel IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF).

3.9
Fertigkeit
Fähigkeit, eine Aufgabe oder Tätigkeit mit einem bestimmten beabsichtigten Ergebnis auszuführen, die durch Ausbildung, Schulung, Erfahrung oder andere Mittel erworben wurde

Anmerkung 1 zum Begriff: Ein Beispiel für eine Fertigkeit ist die Fähigkeit, die mit einem Projekt verbundenen Risiken zu identifizieren und zu klassifizieren.

[QUELLE: ISO/IEC 17027:2014, 2.74, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt.]

4 Konzepte

Um die Konformität bei der Evaluierung oder Konformitätsprüfung von IT-Sicherheitsprodukten zu unterstützen, ist ein Faktor die Kompetenz der Personen, die die Evaluierungs- oder Konformitätsprüfungsarbeiten durchführen. Trotz der Bereitstellung von genormten Konformitätsprüfungs- oder Evaluierungsverfahren ist eine Mindestkompetenz bei der Durchführung der erforderlichen Tätigkeiten erforderlich, um die Konformität und Wiederholbarkeit der Ergebnisse zu unterstützen. Dies wiederum unterstützt die gegenseitige Anerkennung von Zertifizierungen und Validierungen der Vertrauenswürdigkeit von IT-Produkten.

ISO/IEC 17025 befasst sich mit den allgemeinen Anforderungen an die Kompetenz von Prüfungs- und Kalibrierungslaboratorien und wird häufig als Grundlage für die Konformität unter Laboratorien zur Prüfung und Evaluierung der Konformität mit der Vertrauenswürdigkeit angegeben.

Die ISO/IEC 17025 enthält mehrere Anforderungen an die Kompetenz, die von einem Laboratorium erfüllt werden müssen. Diese umfassen:

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 19896-1:2022-10