

DIN EN ISO/IEC 15408-4



ICS 35.030

Einsprüche bis 2024-01-10

Entwurf**Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre –
Evaluationskriterien für IT-Sicherheit –****Teil 4: Rahmen für die Festlegung von Bewertungsmethoden und
-tätigkeiten (ISO/IEC 15408-4:2022);****Deutsche und Englische Fassung prEN ISO/IEC 15408-4:2023**

Information security, cybersecurity and privacy protection –

Evaluation criteria for IT security –

Part 4: Framework for the specification of evaluation methods and activities

(ISO/IEC 15408-4:2022);

German and English version prEN ISO/IEC 15408-4:2023

Sécurité de l'information, cybersécurité et protection de la vie privée –

Critères d'évaluation pour la sécurité des technologies de l'information –

Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités
connexes (ISO/IEC 15408-4:2022);

Version allemande et anglaise prEN ISO/IEC 15408-4:2023

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2023-11-10 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument 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.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 50 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 15408-4:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 15408-4:2023 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 Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. 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 15408-1	siehe	DIN EN ISO/IEC 15408-1
ISO/IEC 15408-2	siehe	DIN EN ISO/IEC 15408-2
ISO/IEC 15408-3	siehe	DIN EN ISO/IEC 15408-3
ISO/IEC 15408-5:2022	siehe	DIN EN ISO/IEC 15408-5:2024-02*
ISO/IEC 17025	siehe	DIN EN ISO/IEC 17025
ISO/IEC 18045	siehe	DIN EN ISO/IEC 18045*
ISO/IEC 19896-3	siehe	DIN EN ISO/IEC 19896-3*

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

* Zurzeit Entwurf.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 15408-1, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell*

DIN EN ISO/IEC 15408-2, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Teil 2: Sicherheitsfunktionskomponenten*

DIN EN ISO/IEC 15408-3, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Teil 3: Sicherheit Gewährleistungskomponenten*

DIN EN ISO/IEC 15408-5:2024-02, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Teil 5: Vordefinierte Pakete von Sicherheitsanforderungen (ISO/IEC 15408-5:2022); Deutsche und Englische Fassung prEN ISO/IEC 15408-5:2023*

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

DIN EN ISO/IEC 18045, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Methodik für die Bewertung der IT-Sicherheit*

DIN EN 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*

– *Entwurf* –

E DIN EN ISO/IEC 15408-4:2023-12

– Leerseite –

**Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre –
Evaluationskriterien für IT-Sicherheit – Teil 4: Rahmen für die Festlegung von
Bewertungsmethoden und -tätigkeiten (ISO/IEC 15408-4:2022)**

Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 4: Framework for the specification of evaluation methods and activities (ISO/IEC 15408-4:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information – Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités connexes (ISO/IEC 15408-4:2022)

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Allgemeines Modell der Evaluierungsmethoden und Evaluierungsaufgaben	8
4.1 Konzepte und Modell	8
4.2 Ableiten von Evaluierungsmethoden und Evaluierungsaufgaben	10
4.3 Verwendung von Verben bei der Beschreibung von Evaluierungsmethoden und Evaluierungsaufgaben	13
4.4 Konventionen für die Beschreibung von Evaluierungsmethoden und Evaluierungsaufgaben	13
5 Aufbau einer Evaluierungsmethode	13
5.1 Übersicht	13
5.2 Spezifikation einer Evaluierungsmethode	14
5.2.1 Übersicht	14
5.2.2 Identifizierung von Evaluierungsmethoden	16
5.2.3 Zuständige Entität für die Evaluierungsmethode	16
5.2.4 Anwendungsbereich der Evaluierungsmethode	16
5.2.5 Abhängigkeiten	17
5.2.6 Erforderliche Eingaben seitens des Entwicklers oder anderer Entitäten	17
5.2.7 Erforderliche Werkzeugarten	17
5.2.8 Erforderliche Kompetenzen des Evaluators	17
5.2.9 Anforderungen an die Berichterstattung	18
5.2.10 Begründung für die Evaluierungsmethode	18
5.2.11 Zusätzliche Verbdefinitionen	20
5.2.12 Eine Reihe von Evaluierungsaufgaben	20
6 Struktur der Evaluierungsaufgaben	20
6.1 Übersicht	20
6.2 Spezifikation einer Evaluierungsaufgabe	20
6.2.1 Eindeutige Identifizierung der Evaluierungsaufgabe	20
6.2.2 Zielsetzung der Evaluierungsaufgabe	21
6.2.3 Verknüpfungen der Evaluierungsaufgaben mit SFR, SAR und anderen Evaluierungsaufgaben	21
6.2.4 Erforderliche Eingaben seitens des Entwicklers oder anderer Entitäten	21
6.2.5 Erforderliche Werkzeugarten	21
6.2.6 Erforderliche Kompetenzen des Evaluators	21
6.2.7 Bewertungsstrategie	22
6.2.8 Bestanden/nicht bestanden-Kriterien	22
6.2.9 Anforderungen an die Berichterstattung	23
6.2.10 Begründung für die Evaluierungsaufgabe	23
Literaturhinweise	25

Bilder

Bild 1 — Zuordnung der Strukturen von ISO/IEC 15408-3 und ISO/IEC 18045 zu den Strukturen des vorliegenden Dokuments	9
---	----------

Bild 2 — Alternative Ansätze zur Zuordnung der ISO/IEC 18045 auf abgeleitete Evaluierungsaufgaben	11
Bild 3 — Inhalt einer Evaluierungsmethode	15

Tabellen

Tabelle 1 — Verteilung des Inhalts zwischen Evaluierungsmethode (EM) und Evaluierungsaufgaben (EA)	15
---	-----------

Europäisches Vorwort

Der Text von ISO/IEC 15408-4:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als prEN ISO/IEC 15408-4:2023 übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

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 abrufbar.

Anerkennungsnotiz

Der Text von ISO/IEC 15408-4:2022 wurde von CEN als prEN ISO/IEC 15408-4:2023 ohne irgendeine Abänderung genehmigt.

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.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC Directives, 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 Directives, Teil 2, erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

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) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe <https://patents.iec.ch>).

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. In der IEC siehe www.iec.ch/understanding-standards.

Dieses Dokument wurde vom Technischen Komitee ISO/TC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection*, erarbeitet.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 15408 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 und www.iec.ch/national-committees zu finden.

Rechtliche Hinweise

Die unten aufgeführten Regierungsorganisationen haben zu der Entwicklung dieser Version der „Common Criteria for Information Technology Security Evaluations“ beigetragen. Als gemeinsame Urheberrechtsinhaber an den Common Criteria for Information Technology Security Evaluations (kurz CC) erteilen sie hiermit der ISO/IEC die nicht-exklusive Lizenz zur Verwendung der CC für die weitere Entwicklung/Pflege der Normenreihe ISO/IEC 15408. Diese Regierungsorganisationen behalten sich allerdings das Recht zur Nutzung, Vervielfältigung, zum Vertrieb sowie zur Übersetzung und Änderung der CC nach Belieben vor.

Australien	The Australian Signals Directorate
Kanada	Communications Security Establishment
Frankreich	Agence Nationale de la Sécurité des Systèmes d'Information
Deutschland	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Niederlande	Netherlands National Communications Security Agency
Neuseeland	Government Communications Security Bureau
Republik Korea	National Security Research Institute
Spanien	Ministerio de Asuntos Económicos y Transformación Digital
Schweden	FMV, Swedish Defence Materiel Administration
Vereinigtes Königreich	National Cyber Security Centre
USA	The National Security Agency

Einleitung

Die Normenreihe ISO/IEC 15408 ermöglicht die Vergleichbarkeit der Ergebnisse unabhängiger Sicherheitsevaluierungen durch eine einheitliche Reihe von Anforderungen an die Sicherheitsfunktionalität von IT-Produkten und an Maßnahmen zur Zusicherung der Vertrauenswürdigkeit, die auf diese IT-Produkte während einer Sicherheitsevaluierung angewendet werden. ISO/IEC 18045 bietet eine begleitende Methodologie für einige der in der Normenreihe ISO/IEC 15408 festgelegten Vertrauenswürdigkeitsanforderungen.

Das Modell der Sicherheitsevaluierung in ISO/IEC 15408-1 legt fest, dass allgemeine generische Evaluierungsaufgaben in ISO/IEC 18045 definiert sind, dass aber spezifischere Evaluierungsaufgaben (EA) als technologie-spezifische Anpassungen dieser generischen Aufgaben für bestimmte Evaluierungskontexte definiert werden können, z. B. für Sicherheitsfunktionsanforderungen (SFR) oder Vertrauenswürdigkeitsanforderungen (SAR), die auf bestimmte Technologien oder Typen von Evaluierungsgegenständen (TOE) angewendet werden. Solche Evaluierungsaufgaben werden in der Praxis bereits spezifiziert, sodass ein Bedarf an einer Spezifikation für die Definition solcher Evaluierungsaufgaben besteht.

Dieses Dokument beschreibt einen Rahmen, der für die Ableitung von Evaluierungsaufgaben aus den Workunits der ISO/IEC 18045 und deren Bündelung in Evaluierungsmethoden (EM) verwendet werden kann. Evaluierungsaufgaben oder -methoden können in die Schutzprofile (PP) und alle sie unterstützenden Dokumente aufgenommen werden. Wenn in einem PP, einer PP-Konfiguration, einem PP-Modul, einem Paket oder in den Sicherheitsvorgaben (ST) festgelegt ist, dass bestimmte Evaluierungsmethoden/Evaluierungsaufgaben zu verwenden sind, müssen die Evaluatoren nach ISO/IEC 18045 die entsprechenden Evaluierungsmethoden/Evaluierungsaufgaben bei der Zuordnung von Evaluatoren-Entscheidungen befolgen und melden. Wie in ISO/IEC 15408-1 erwähnt, kann eine Evaluierungsinstanz in einigen Fällen entscheiden, die Anwendung bestimmter Evaluierungsmethoden/Evaluierungsaufgaben nicht zu genehmigen: In einem solchen Fall kann die Evaluierungsinstanz entscheiden, keine Evaluierungen in Anlehnung an eine ST durchzuführen, die diese Evaluierungsmethoden/Evaluierungsaufgaben erfordert.

Das vorliegende Dokument lässt auch die Definition von Evaluierungsaufgaben für erweiterte SAR zu. In diesem Fall bezieht sich die Ableitung der Evaluierungsaufgaben auf gleichwertige Aktionselemente und Workunits, die für die jeweilige erweiterte SAR definiert wurden. Wenn in diesem Dokument auf die Verwendung von ISO/IEC 18045 oder ISO/IEC 15408-3 für die SAR verwiesen wird (z. B. bei der Definition von Begründungen für Evaluierungsaufgaben), dann gilt die Verweisung im Falle einer erweiterten SAR stattdessen für die entsprechenden Aktionselemente und Workunits, die für diese erweiterte SAR definiert wurden.

Aus Gründen der Klarheit spezifiziert dieses Dokument, wie Evaluierungsmethoden und Evaluierungsaufgaben zu definieren sind, gibt aber selbst keine Beispiele für Evaluierungsmethoden oder Evaluierungsaufgaben.

Die folgende Anmerkung erscheint in anderen Teilen der Normenreihe ISO/IEC 15408 und in ISO/IEC 18045, um die Verwendung von fetter und kursiver Schrift in diesen Dokumenten zu beschreiben. In diesem Dokument werden diese Konventionen nicht verwendet, aber die Anmerkung wurde beibehalten, um eine Einheitlichkeit im Hinblick auf die anderen Teile der Normenreihe sicherzustellen.

ANMERKUNG Im vorliegenden Dokument werden einige Begriffe fett und kursiv gedruckt, um sie vom übrigen Text abzuheben. Die Beziehung zwischen den Komponenten einer Familie wird als Konvention über eine Fettmarkierung hervorgehoben. Diese Markierungskonvention erfordert die Verwendung von Fettdruck für alle neuen Anforderungen. Für hierarchische Komponenten werden Anforderungen fett hervorgehoben, wenn sie über die Anforderungen der vorherigen Komponente hinaus erweitert oder geändert werden. Zusätzlich werden alle neuen oder erweiterten zulässigen, über die vorherige Komponente hinausgehenden Operationen ebenfalls fett hervorgehoben.

Die Verwendung von Kursivschrift weist auf einen Text hin, der eine genaue Bedeutung hat. Für die Vertrauenswürdigkeitsanforderungen gilt die Konvention für spezielle Verben, die sich auf die Evaluierung beziehen.

1 Anwendungsbereich

Dieses Dokument bietet einen standardisierten Rahmen für die Spezifikation objektiver, wiederholbarer und reproduzierbarer Evaluierungsmethoden und Evaluierungsaufgaben.

In diesem Dokument wird nicht spezifiziert, wie Evaluierungsmethoden und Evaluierungsaufgaben zu evaluieren, zu übernehmen oder zu pflegen sind. Diese Aspekte fallen in den Zuständigkeitsbereich derjenigen, die die Evaluierungsmethoden und die Evaluierungsaufgaben in ihrem jeweiligen Interessengebiet entwickeln.

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 15408-1, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Methodology for IT security evaluation*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3 und ISO/IEC 18045.

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 <https://www.electropedia.org/>

4 Allgemeines Modell der Evaluierungsmethoden und Evaluierungsaufgaben

4.1 Konzepte und Modell

ISO/IEC 18045 definiert eine generische Reihe von Workunits, die ein Evaluator ausführt, um zu einer Entscheidung für die meisten der in ISO/IEC 15408-3 definierten Vertrauenswürdigkeitsklassen, -familien und -komponenten zu gelangen. Die Beziehung zwischen dem Aufbau einer SAR in ISO/IEC 15408-3 und den Workunits in ISO/IEC 18045 wird in ISO/IEC 18045 beschrieben und ist in Bild 1 zusammengefasst.

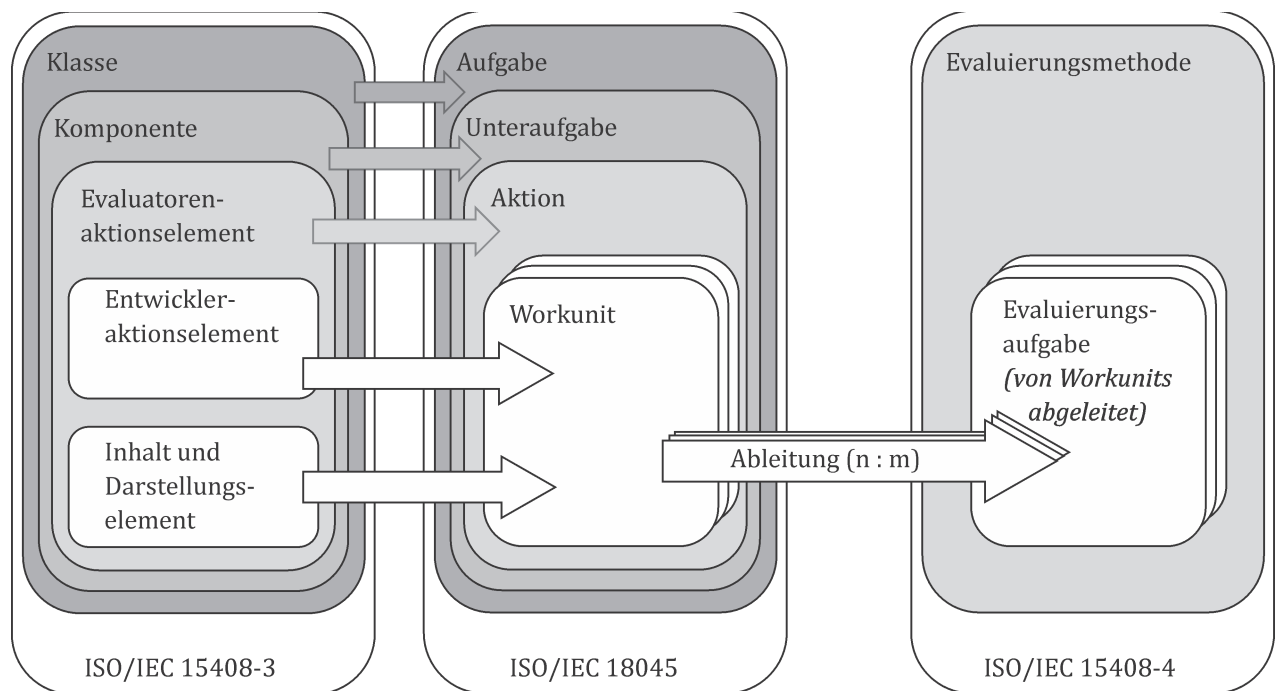


Bild 1 — Zuordnung der Strukturen von ISO/IEC 15408-3 und ISO/IEC 18045 zu den Strukturen des vorliegenden Dokuments

Für die Zwecke der Definition neuer Evaluierungsmethoden und Evaluierungsaufgaben ist vor allem zu beachten, dass jede Aktion (die ein Evaluatorenaktionselement in ISO/IEC 15408-3 oder ein impliziertes Evaluatorenaktionselement darstellt) in ISO/IEC 18045 als eine Reihe von Workunits dargestellt wird, die von einem Evaluator durchgeführt werden.

Dieses Dokument legt fest, wie neue Evaluierungsaufgaben aus den generischen Workunits in ISO/IEC 18045 abgeleitet und zu einer Evaluierungsmethode kombiniert werden können, die für den Einsatz in einem bestimmten Evaluierungskontext vorgesehen ist. Ein typisches Beispiel für einen solchen Evaluierungskontext wäre ein bestimmter TOE-Typ oder ein bestimmter Technologietyp.

BEISPIEL 1

TOE-Typ: ein Netzwerkgerät

Technologietyp: spezifische kryptographische Funktionen

Wenn für ein bestimmtes PP, ein PP-Modul oder eine PP-Konfiguration Evaluierungsmethoden und Evaluierungsaufgaben vorgeschrieben sind, dann muss ein PP, ein PP-Modul oder eine PP-Konfiguration diese Anforderung in ihrer Konformitätserklärung bestimmen. Wenn für ein bestimmtes Paket Evaluierungsmethoden und Evaluierungsaufgaben vorgeschrieben sind, dann muss das Paket diese Anforderung im Abschnitt „Sicherheitsanforderungen“ bestimmen. Wenn Evaluierungsmethoden und Evaluierungsaufgaben von einer ST beansprucht werden, weil diese ST die Konformität mit einem PP, einer PP-Konfiguration oder einem Paket beansprucht, dann muss die ST die in ihrem Konformitätsanspruch verwendeten EM/EA bestimmen. In keinem dieser Fälle wird ein formaler Anspruch auf Konformität mit ISO/IEC 15408-4 erhoben (die Inhalte der PP, PP-Module, PP-Konfigurationen und Pakete sind in ISO/IEC 15408-1 ausführlicher beschrieben).

Ein PP, eine PP-Konfiguration, ein PP-Modul oder ein Paket darf mehr als eine Evaluierungsmethode oder eine separate Reihe von Evaluierungsaufgaben verwenden.

BEISPIEL 2 Es können mehrere Evaluierungsmethoden verwendet werden, wenn getrennte Evaluierungsmethoden für kryptographische Operationen und für sichere Kanalprotokolle, die in einem PP verwendet werden, definiert wurden.

ANMERKUNG Für den Fall, dass genaue Konformität verwendet wird, besagt ISO/IEC 15408-1, dass Evaluierungsmethoden/Evaluierungsaufgaben nicht in einer PP-Konfiguration definiert werden dürfen: Die zu verwendenden Evaluierungsmethoden/Evaluierungsaufgaben sind in den PP und PP-Modulen enthalten und nicht in der PP-Konfiguration).

Wenn ein PP, ein PP-Modul, eine PP-Konfiguration oder ein Paket bestimmt, dass gewisse Evaluierungsmethoden/Evaluierungsaufgaben zu verwenden sind, dann geschieht dies unter Verwendung eines Standardwortlauts, der die Anforderung angibt und auf die Definition der zu verwendenden Evaluierungsmethoden/Evaluierungsaufgaben verweist. Eine ST darf nur die geforderten Evaluierungsmethoden und Evaluierungsaufgaben bestimmen, die in einem PP, PP-Modul, einer PP-Konfiguration oder einem Paket enthalten sind, für das bzw. die die ST Konformität beansprucht (d. h. die ST selbst darf keine Evaluierungsmethoden oder Evaluierungsaufgaben hinzufügen, ändern oder entfernen). Eine ST muss alle erforderlichen Evaluierungsmethoden/Evaluierungsaufgaben aufführen (d. h. einschließlich derjenigen, die von den PP, PP-Modulen, PP-Konfigurationen oder Paketen, mit denen die ST Konformität beansprucht, gefordert werden), sodass es eine einzige Liste gibt, die von Evaluatoren und Lesern der ST überprüft und herangezogen werden kann.

Evaluierungsmethoden und Evaluierungsaufgaben dürfen innerhalb des Dokuments, das sie vorschreibt (z. B. als Teil eines PP), oder extern in einem anderen Dokument (oder in einer Kombination aus beidem) definiert werden. Obwohl die Identifizierung wie oben beschrieben erforderlich ist, ist es nicht notwendig, den Text der Evaluierungsmethoden/Evaluierungsaufgaben in anderen Dokumenten wiederzugeben (z. B. muss eine ST nicht den vollständigen Text der Evaluierungsmethoden/Evaluierungsaufgaben aus einem PP enthalten, für das sie Konformität beansprucht).

4.2 Ableiten von Evaluierungsmethoden und Evaluierungsaufgaben

Im Allgemeinen darf die Festlegung von Evaluierungsaufgaben und -methoden entweder von einer SAR ausgehen, mit dem Ziel, einige oder alle Teile ihrer Workunits näher zu spezifizieren, oder von einer SFR, mit dem Ziel, spezifische Aspekte von Workunits im Zusammenhang mit dieser SFR zu definieren.

Ausgehend von einer SAR gilt als Leitlinie für den Prozess Folgendes:

- a) Identifizieren der relevanten Workunits nach ISO/IEC 18045, aus denen mindestens eine einzelne Evaluierungsaufgabe oder eine Gruppe von Evaluierungsaufgaben abgeleitet werden soll.
- b) Für jede Workunit, aus der eine Evaluierungsaufgabe abgeleitet wird:
 - 1) Definieren der neuen Evaluierungsaufgaben im Hinblick auf die durchzuführenden spezifischen Arbeiten und die in 6.2 beschriebenen Evaluationskriterien (unter Umständen einschließlich der in 6.2.8 beschriebenen Kriterien für die Ergebnisse Bestanden/Nicht bestanden).
 - 2) Bündeln von Evaluierungsaufgaben zu einer Evaluierungsmethode, falls erforderlich.
 - 3) Begründen der neuen Evaluierungsaufgaben und der Evaluierungsmethode, unter der sie wie in 5.2.10 und 6.2.10 beschrieben gebündelt werden.

BEISPIEL Eine Begründung kann eine Verweisung auf die Entwickleraktion sowie auf die Inhalts- und Darstellungselemente der Workunits enthalten, von denen sie abgeleitet sind.

Eine Leitlinie zum Start ausgehend von einer SFR würde wie folgt lauten:

- a) Bestimmen der relevanten SFR.
- b) Bestimmen der SAR (aus ISO/IEC 15408-3 oder einer Reihe erweiterter SAR oder beidem), die für diese spezielle SFR angesprochen werden sollen, und der entsprechenden Workunits nach ISO/IEC 18045.
- c) Definieren der neuen Evaluierungsaufgaben im Hinblick auf die durchzuführenden spezifischen Arbeiten und die in 6.2 beschriebenen Evaluationskriterien (einschließlich, falls erforderlich, der in 6.2.8 beschriebenen bestanden/nicht bestanden-Kriterien).

BEISPIEL Evaluierungsaufgaben können definiert werden, um die Darstellung einer bestimmten SFR in der zusammenfassenden Spezifikation des TOE zu untersuchen (abgeleitet von ASE), um die Darstellung der SFR in der Leitliniendokumentation zu untersuchen (abgeleitet von AGD), und um spezifische Prüfungen der SFR durchzuführen (abgeleitet von ATE).

- d) Zuordnen der betroffenen Workunits für die SAR zu den neuen Evaluierungsaufgaben.
- e) Begründen der neuen Evaluierungsaufgaben und der Evaluierungsmethode, unter der sie wie in 5.2.10 und 6.2.10 beschrieben gebündelt werden.

Obwohl ein Autor wählen darf, ob er von den SAR oder den SFR ausgeht, ist zu beachten, dass die SAR letztlich alle SFR abdecken. Die oben beschriebene Methode, von den SFR auszugehen, kann nützlich sein, wenn es darum geht, zu klären, wie eine SAR auf eine bestimmte SFR anwendbar ist, und sie kann nützlich sein, um die SFR zusammen mit der Beschreibung ihrer Evaluierungsaufgaben darzustellen.

Eine 1 : 1-Zuordnung von Workunits zu neuen Evaluierungsaufgaben ist nicht erforderlich, und die tatsächliche Übereinstimmung wird in einer Begründung dokumentiert (wie in 5.2.10 beschrieben). Die Ableitung kann in Bezug auf einzelne Workunits oder Gruppen von Workunits erfolgen, was in Bild 2 dargestellt ist. Im Fall a) von Bild 2 ordnet der Autor jede Workunit aus ISO/IEC 18045 einer entsprechenden Evaluierungsaufgabe zu, während im Fall b) der Autor eine unterschiedliche Anzahl von Workunits und Evaluierungsaufgaben zuordnet, wobei er dennoch alle Aspekte einer Aktion (d. h. die Sammlung von Workunits) berücksichtigt.

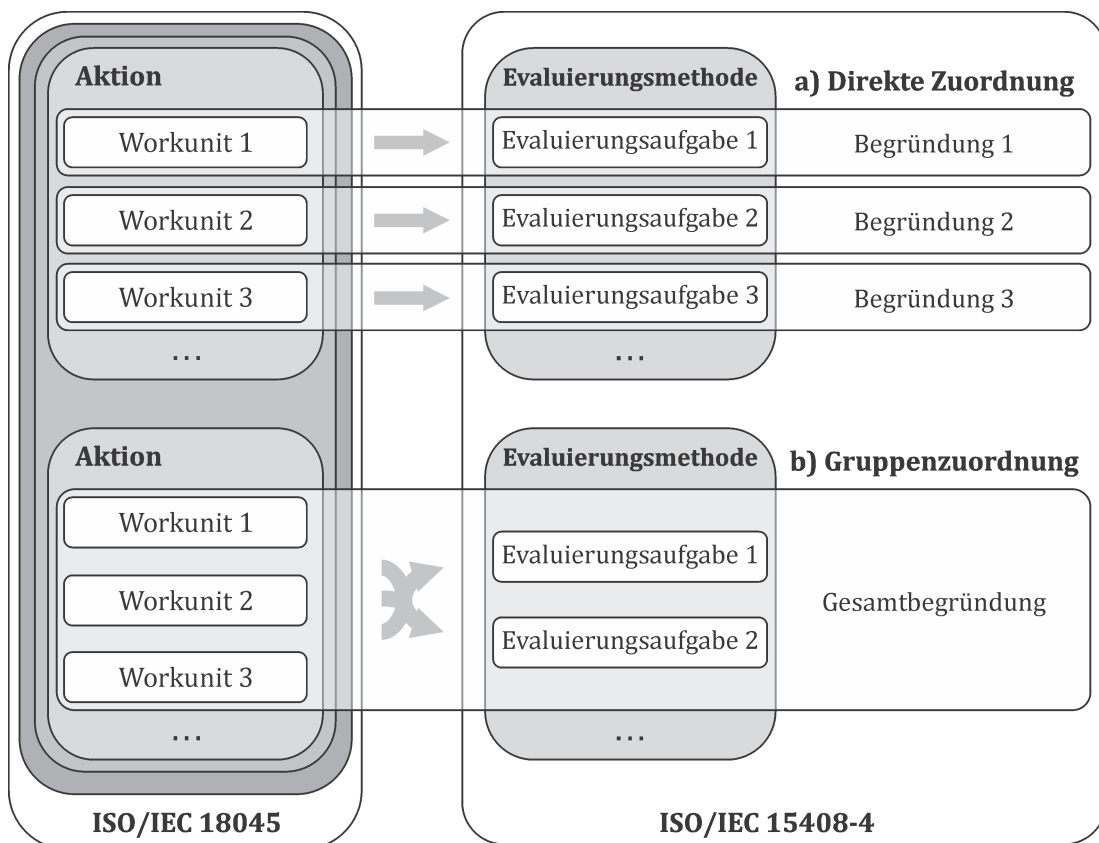


Bild 2 — Alternative Ansätze zur Zuordnung der ISO/IEC 18045 auf abgeleitete Evaluierungsaufgaben

Je nach Inhalt der spezifischen Workunits und Evaluierungsaufgaben sind auch andere Ansätze möglich: Selbst wenn die gleiche Anzahl von Workunits und Evaluierungsaufgaben vorhanden ist, ist eine einfache 1 : 1-Zuordnung manchmal nicht möglich, sodass eine Zuordnung auf der Ebene der Aktionen angemessen sein kann. Einige detailliertere Zuordnungssituationen werden in den folgenden Beispielen beschrieben.