

Prüfkatalog vertrauenswürdige KI-Systeme: BSI veröffentlicht Community Draft des A5

5.10.2026 - | Bundesamt für Sicherheit in der Informationstechnik

Mit der Entwicklung der AI Audit and Assurance Assessment Architecture (A5) legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Grundstein für eine modulare und erweiterbare Prüfarchitektur für KI-Systeme. Das BSI hat den A5 als Community Draft zur Kommentierung veröffentlicht. A5 richtet sich an alle Akteure entlang der KI-Wertschöpfungskette, von Anbietern über Betreiber bis hin zu den mit Entwicklung, Betrieb und Aufsicht betrauten Personen. Anmerkungen und Anregungen können bis zum 31. August 2026 über den Kommentierungsbogen per E-Mail an aisecurity@bsi.bund.de geschickt werden.

Künstliche Intelligenz kommt in immer mehr Bereichen zum Einsatz und transformiert dabei Staat, Wirtschaft und Gesellschaft nachhaltig. Mit wachsender Verbreitung und Komplexität von KI-Systemen gibt es auch mehr regulatorische Anforderungen für deren Verwendung. Zentral für die Informationssicherheit ist dabei der Nachweis der Vertrauenswürdigkeit von KI-Systemen. Genau dort setzt der A5 an und unterstützt Stakeholder mit Kriterien und Methodik bei der systematischen und standardisierten Bewertung. Im Kontext regulatorischer Anforderungen wie EU AI Act und Cyber Resilience Act sowie weiterer Standards bietet der A5 einen Rahmen, um technische Vertrauenswürdigkeit nachvollziehbar zu transportieren.

Die A5-Kriterien orientieren sich an den strukturellen Konventionen der Stand-der-Technik-Bibliothek des BSI und werden auch dokumentenbasiert und maschinenlesbar im internationalen Standard für Sicherheitsanforderungen (OSCAL) umgesetzt. Nutzerinnen und Nutzer können die A5-Kriterien in bestehende OSCAL-basierte Werkzeuge zur Compliance-Bearbeitung und Prüfunterstützung einbinden.

Das BSI hat erste A5-Kriterien, die einen technologie- und anwendungsunabhängigen Prüfkontext adressieren, als horizontales Basismodul zusammengestellt. Zur initialen Bereitstellung einer A5-Prüfmethodik orientiert sich das BSI an der Methodik des C5 (Cloud Computing Compliance Criteria Catalog), die sich auf den International Standard on Assurance Engagements 3000 (ISAE 3000) stützt. Dieser gilt als international etablierter Prüfstandard. Über das Betriebsmodul Cloud-Infrastruktur des A5 gibt es auch eine zentrale Querverbindung zum C5-Katalog des BSI.

Der A5 wurde im Rahmen des BSI-Projekts "AICRID - Entwicklung von Prüfkriterien und Prüfmethoden für KI-Systeme" erarbeitet und berücksichtigt dabei sowohl inhaltliche Erkenntnisse aus diversen nationalen und internationalen Standards, Best Practices und Regelwerken als auch Ergebnisse aus weiteren BSI-Projekten. Das BSI aktualisiert, erweitert und erprobt den A5 kontinuierlich, um den dynamischen und komplexen Entwicklungen im Bereich KI zu begegnen. Mit dem A5 leistet das BSI einen entscheidenden Beitrag, die Vertrauenswürdigkeit künstlicher Intelligenz zu überprüfen.

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260706_KI_A5-Community-Draft.html