

KPMG zertifiziert ersten KI-Agenten nach AIUC-1: Was es bedeutet

MANAGEMENT SUMMARY & KERNAUSSAGE

KPMG hat im September 2026 als erste Big-Four-Firma einen KI-Agenten offiziell nach AIUC-1 zertifizieren lassen: über 900 Tests, keine kritischen Schwachstellen. Für Schweizer KMU zeigt der Fall, welche Prüftiefe produktionsreife KI-Agenten heute erreichen können – und dass Governance und Risikoeinschätzung vor jeder Zertifizierung stehen müssen.

KONTEXT & RELEVANZ FÜR ENTSCHEIDER

Im September 2026 hat KPMG als erste der vier grossen Prüfungs- und Beratungsgesellschaften einen eigenen KI-Agenten nach dem neuen AIUC-1-Standard zertifizieren lassen. Der Agent heisst alQ Capture und wandelt Sprachinterviews in strukturierte Kundenerkenntnisse um. Die Prüfung umfasste mehr als 900 Einzeltests – von Halluzinationsauslösern über Hochrisiko-Domänen bis zu Content-Sicherheit und Prompt-Injection-Angriffen. Das Ergebnis: keine kritischen oder schwerwiegenden Schwachstellen. Für ein autonomes System, das eigenständig Entscheidungen trifft und Werkzeuge aufruft, ist das ein bemerkenswert dichtes Testraster.

Die meisten bisherigen KI-Zertifizierungen prüfen Modelle oder Managementsysteme. AIUC-1 ist anders konzipiert: Der Standard zielt gezielt auf agentische Systeme ab – also auf KI, die nicht nur Text generiert, sondern autonom handelt, Werkzeuge aufruft und Entscheidungen trifft. Genau das macht ihn für Versicherer interessant. Zum ersten Mal gibt es einen Prüfraum, der als Grundlage für die Versicherbarkeit autonomer Systeme taugt – relevant für jeden Einsatz in regulierten oder kundennahen Bereichen.

KERN-HANDLUNGSEMPFEHLUNGEN

- 01 Investitionslücke: Unternehmen stecken laut Gartner rund achtmal mehr Budget in neue Agentenfähigkeiten als in deren Kontrolle und Überwachung.
- 02 Datenqualität als Flaschenhals: In rund 85 Prozent der Fälle scheitert die Skalierung laut Gartner nicht an der KI, sondern an unzureichender Datenbasis.
- 03 Kaufen schlägt Bauen: Die MIT-NANDA-Studie zeigt eine Erfolgsquote von 67 Prozent bei extern beschafften Agentenlösungen gegenüber 33 Prozent bei Eigenentwicklung.

SCHWEIZER UMSETZUNGSKRITERIEN (REVDSG & IT-ARCHITEKTUR)

- ☒ Vollständige Konformität mit dem neuen Schweizer Datenschutzgesetz (revDSG).
- ☒ Keine Abhängigkeiten: Zero Lock-In auf proprietäre geschlossene Modelle.
- ☒ Schnittstellen zu Schweizer ERPs (Abacus, Bexio, M365) im operativen Betrieb.

Unverbindliche Prozess-Analyse

Lass uns in 20 Minuten prüfen, wo KI-Agenten in deinem Unternehmen sofort messbare Entlastung schaffen.

ki-outsourcing.ch