

Die eingereichten Fragen werden vom BSI in diesem Dokument beantwortet und als PDF-Dokument veröffentlicht. Das Dokument daher bitte nicht bereits im Vorfeld in ein PDF-Dokument umwandeln!

Lfd. Nr.	Dokument (*)	Seite	Kapitel	Textstelle	Frage	Antwort
7	Leistungsbeschreibung	29	6.2.1.3, Nr. 2 bis 5		Gehen wir recht in der Annahme, dass auch laufende Projekte als Unternehmensreferenzen anerkannt werden?	Ja.
8	Leistungsbeschreibung	29	6.2.1.3, Nr. 3		Bezugnehmend auf die Unternehmensreferenz „Expertise zur Prüfung von KI-Systemen“: Wir bitten um Klarstellung, welche Art der Prüfung hier gefordert ist bzw. auf welche Aspekte sich die geforderte Expertise zur Prüfung von KI-System beziehen soll.	Ein Auftragnehmer kann seine Expertise zur Prüfung von KI-Systemen, die auf die in 2.3 genannten Kriterien abstellt, beispielsweise durch Referenzprojekte belegen, also bereits durchgeführte Prüfungen vergleichbarer Systeme mit dokumentierter Methodik und aussagekräftigen Prüfberichten. Ergänzend zählen Fachpublikationen, Konferenzvorträge sowie Mitwirkung an einschlägigen Standards und Gremien. Praktische Angriffskompetenz lässt sich durch verantwortungsvoll gemeldete Schwachstellen oder Beiträge zu anerkannten Prüfwerkzeugen nachweisen. Auch übertragbare Qualifikationen aus der klassischen IT-Sicherheitsprüfung (z. B. Pentest-Zertifikate, Erfahrung mit IT-Grundschutz oder C5) sind relevant, sofern eine dokumentierte KI-Spezialisierung hinzukommt. Zentral ist zudem eine nachvollziehbare, dokumentierte Prüfmethodik mit klaren Bedrohungsmodellen, Testverfahren und Berichtsstandards. Da formale Zertifizierungen für KI-Prüfungen noch nicht verbreitet

Lfd. Nr.	Dokument (*)	Seite	Kapitel	Textstelle	Frage	Antwort
						sind, ist die Kombination dieser Nachweise derzeit der aussagekräftigste Eignungsbeleg.
10	Leistungsbeschreibung	29	6.2.1.3, Nr. 4		Bezugnehmend auf die Unternehmensreferenz „Expertise zu Sicherheit von KI-Systemen“: Wir bitten um Klarstellung, auf welcher Ebene die Expertise zur Sicherheit von KI-Systemen nachgewiesen werden soll.	Ein Auftragnehmer kann seine Expertise zur Sicherheit von KI-Systemen beispielsweise durch Referenzprojekte belegen, in denen er (agentische) KI-Systeme sicher konzipiert, gehärtet oder abgesichert hat – etwa durch dokumentierte Sicherheitsarchitekturen und umgesetzte Schutzmaßnahmen für (agentische) KI-Systeme. Weiterführend sind Fachpublikationen, Konferenzvorträge sowie Mitwirkung an einschlägigen Standards und Rahmenwerken relevant. Die nachweisbare Anwendung anerkannter Sicherheitsprinzipien zu agentischer KI in realen Projekten ist dabei aussagekräftiger als rein theoretisches Wissen. Auch Beiträge zu Open-Source-Sicherheitswerkzeugen oder verantwortungsvoll gemeldete Schwachstellen belegen ein tiefes technisches Verständnis über Angriffe. Übertragbare Qualifikationen aus der klassischen IT-Sicherheit sind relevant, sofern eine dokumentierte KI-Spezialisierung hinzukommt. Da formale Zertifizierungen in diesem Bereich noch nicht verbreitet sind, ist die Kombination dieser Nachweise derzeit der aussagekräftigste Eignungsbeleg.

Lfd. Nr.	Dokument (*)	Seite	Kapitel	Textstelle	Frage	Antwort
11	Leistungsbeschreibung	33-34	6.2.1.4, Nr. 1.3 bis 1.5		Bezugnehmend auf die qualitativen Zuschlagskriterien (Nr. 1.3 bis 1.5): Gehen wir recht in der Annahme, dass für die einzureichenden Konzepte keine formalen Vorgaben, insbesondere hinsichtlich Seitenumfang, Schriftart oder Schriftgröße, bestehen?	Es bestehen keine formalen Vorgaben für die einzureichenden Konzepte zu den Zuschlagskriterien.
5						

(*) Leistungsbeschreibung, Projektvertrag, Bekanntmachung, allgemeine Frage, etc.