



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Projekt 1008

KI im Secure Software Development Life Cycle (KISDL)

Leistungsbeschreibung und Besondere Bewerbungsbedingungen

Version: 1.0

Datum: 03.08.2026



Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: <https://www.bsi.bund.de>
© Bundesamt für Sicherheit in der Informationstechnik 2026

Inhaltsverzeichnis

A	Leistungsbeschreibung	5
1	Übersichtsinformationen zum Projekt	5
1.1	Auftraggeber (AG).....	5
1.2	Ausgangslage und Handlungsbedarf	5
1.3	Auftragsgegenstand und Projektziele.....	6
1.4	Projektstrukturplan.....	8
2	Beschreibung der Arbeitspakete	9
2.1	Arbeitspaket 1: Auftaktbesprechung und Feinkonzept (Auftaktbesprechung).....	9
2.2	Arbeitspaket 2: Ermittlung des Forschungs- und Markstandes zum Thema KI im SSDLC, Vergleich der Methoden und Veröffentlichung der Ergebnisse (Studie zu KI im SSDLC).....	9
2.3	Arbeitspaket 3: Erarbeitung von Best Practices zum Einsatz ausgewählter Tools im SSDLC und Erstellung eines Proof of Concepts (Best Practices und PoC).....	11
2.4	Arbeitspaket 4: Zwischenworkshop zur Vorstellung bisheriger Ergebnisse und Feinkonzept (Zwischenworkshop)	12
2.5	Arbeitspaket 5 (OPTIONAL): Einordnung und Empfehlungen für AVA-Bepunktung in den Common Criteria (Aktualisierung Einordnung CC-Bewertungsmetrik).....	12
2.6	Arbeitspaket 6 (OPTIONAL): Erstellung einer Guideline für den Einsatz von KI-Tools mit Dual-Use in Prüfstellen und ggf. bei Herstellern (Guideline: KI-Tools in der Evaluierung in Prüfstellen).....	14
2.7	Arbeitspaket 7 (OPTIONAL): Erstellung einer Referenzarchitektur für die Integration von KI-Tools des SSDLC in Open CoDE (Referenzarchitektur KI-Tools im SSDLC in Open CoDE).....	15
2.8	Arbeitspaket 8 (OPTIONAL): Abschlusspräsentation der Projektergebnisse und Abschlussbericht (Abschlussworkshop).....	16
3	Zahlungs- und Meilensteinplan, Projektplan und Vergütung	18
3.1	Vergütung.....	18
3.1.1	Vergütung von AP nach Festpreis.....	18
3.1.2	Vergütung von AP nach Aufwand	18
3.1.2.1	Personalkosten.....	18
3.1.2.2	Lizenzkosten	19
3.2	Projektverlauf, Zahlungs- und Meilensteinplan	20
4	Rahmen- und Ausführungsbedingungen.....	22
4.1	Personal des Auftragnehmers	22
4.1.1	Direktionsrecht und Disziplinargewalt	22
4.1.2	Qualifikationen, Erfahrungen und sonstige Anforderungen	22
4.1.3	Personaleinsatz und -austausch.....	23
4.2	Projektorganisation und Erreichbarkeit.....	23
4.3	Projektsprache.....	24
4.4	Besprechungen.....	24
4.5	Berichtswesen.....	24

4.6	Formale Anforderungen an Projektdokumente	24
4.7	Barrierefreie Gestaltung	25
4.8	Verschlüsselung der Kommunikation.....	26
4.9	Berechtigte Interessen des Herstellers	26
4.10	Einsatz von Unterauftragnehmern.....	26
4.11	Anforderungen an die Rechnungsstellung.....	26
4.11.1	Zeitpunkt	26
4.11.2	Elektronische Form.....	27
4.12	Nachhaltige Umsetzung der Leistung	27
B	Besondere Bewerbungsbedingungen	28
5	Bedingungen für die Zuschlagserteilung	28
5.1	Gesetzliche Ausschlussgründe, Eignung und Ausführungsbedingungen.....	28
5.2	Wirtschaftlichstes Angebot.....	28
5.2.1	Bewertungspreis	29
5.2.2	Leistung	29
5.2.3	Erweiterte Richtwertmethode mit dem Entscheidungskriterium „Leistungspunkte“	30
6	Erstellung des Angebots	31
6.1	Angebotsformular.....	31
6.2	Anlagen zum Angebotsformular	31
6.2.1	Anlage: Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen.....	32
6.2.1.1	Einzelbieter / Mitglieder der Bietergemeinschaft.....	32
6.2.1.2	Unterauftragnehmer	32
6.2.1.3	Eignungskriterien	33
6.2.1.4	Qualitative Zuschlagskriterien.....	36
6.2.2	Anlage: Bietergemeinschaftserklärung.....	44
6.2.3	Anlage: Unterauftragnehmerverspflichtungserklärung(en).....	44
6.2.4	Anlage: Angaben zu vorliegenden Ausschlussgründen und zur Selbstreinigung im Sinne von § 125 GWB	45
C	Abkürzungsverzeichnis	46
D	Muster Leistungsnachweis.....	47

A Leistungsbeschreibung

1 Übersichtsinformationen zum Projekt

1.1 Auftraggeber (AG)

Als die Cybersicherheitsbehörde des Bundes gestaltet das Bundesamt für Sicherheit in der Informationstechnik (BSI) Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Das BSI wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Derzeit sind dort ca. 1.650 Mitarbeitende beschäftigt. Seinen Hauptsitz hat das BSI in Bonn.

Das BSI ist die zentrale, unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit. Das BSI schützt die Netze des Bundes; es richtet sich jedoch zugleich auch an gewerbliche und private Anbieter wie Nutzer von Informationstechnik. Das breite Aufgabenspektrum des BSI ist im [BSI-Gesetz](#) geregelt.

1.2 Ausgangslage und Handlungsbedarf

Methoden der Künstlichen Intelligenz (KI) zeigen in vielen Anwendungsbereichen erstaunliche Leistungen und werden zunehmend in Bereichen eingesetzt, die unser tägliches Leben beeinflussen. Auch das Gebiet der Cybersicherheit ist von KI nicht unberührt geblieben. Neue Tools werden beinahe täglich veröffentlicht, und vor allem Große KI-Sprachmodelle (LLMs) werden bereits heute zu diversen Anwendungszwecken eingesetzt. Die Bedrohungslage, z.B. durch Missbrauch von gutartig intendierten Modellen zu Angriffszwecken (Dual Use), wird dadurch stark verändert.

Da LLMs neben natürlichsprachlichen Texten häufig auch Code verarbeiten können, ist die Anwendung zur Codeanalyse naheliegend, z.B. um Schwachstellen zu identifizieren. Quellcode kann aus einer Vielzahl von Gründen Schwachstellen enthalten. So können menschliche Fehler und Unwissenheit die Ursache sein, Schwachstellen möglicherweise zum Zeitpunkt der Entwicklung noch nicht bekannt sein, oder auch Programmierassistenten unsicheren Code vorschlagen, der durch Entwickler unverändert übernommen wird. Werden die Schwachstellen ausgenutzt, können die Schäden verheerend sein. Aus diesem Grund ist es aus Sicht der Cybersicherheit wichtig, dass Code möglichst ohne Schwachstellen entwickelt wird und bestehende Schwachstellen möglichst frühzeitig detektiert und beseitigt werden. Zu diesem Zweck haben sich entsprechende Codeanalysetools im Kontext der Softwareentwicklung etabliert. Allerdings weisen die aktuell verfügbaren Tools einige Schwächen auf. So finden diese Tools häufig nur einen Teil der Schwachstellen, gehen mit hohen False-Positive-Raten einher, die zu hohem Arbeitsaufwand und niedriger Akzeptanz führen, und sind häufig nur von Experten produktiv nutzbar, da sie besondere Kenntnisse zur korrekten Interpretation und Weiterverarbeitung der Ergebnisse erfordern. Es stellt sich deshalb die Frage, inwiefern der Einsatz von KI diese Schwächen mildern oder ganz beseitigen kann.

Die Nutzung von LLMs im Secure Software Development Life Cycle (SSDLC) ist ein aktives Forschungsgebiet. Auch die Industrie ist hieran interessiert und beginnt, KI in derartige Produkte zu integrieren. Zurzeit existiert unseres Wissens nach kein Überblick über die tatsächlichen Fähigkeiten und Potenziale von LLMs in diesem Einsatzgebiet sowie der möglichen Veränderungen, die damit einhergehen (z.B. wie Angreifende durch den Einsatz solcher Tools gestärkt werden). Eine solche Einschätzung, basierend auf belastbaren Daten, ist allerdings essenziell, um beispielsweise geeignete Sicherheitsempfehlungen auszugeben. Zudem könnte ein solches Tool der produktiven Arbeit des BSI und der Bundesverwaltung zu Gute kommen, und die allgemeine Resilienz der Bundesverwaltung erhöhen, indem Schwachstellen schneller und einfacher analysiert und behoben werden können.

Aufbauend auf dieser Ausgangslage zeigt sich ein Handlungsbedarf für das BSI, um seinem Anspruch gerecht zu werden, die aktuelle Cybersicherheitslage korrekt erfasst zu haben und Vorgänge auf der Basis fundierter Daten durchzuführen. Im Einzelnen sind folgende Aufgaben des BSI aus dem BSI-Gesetz (BSIG) hervorzuheben:

- BSIG §3 Absatz 1 Satz 2 Ziffer 1: Gefahren für die Sicherheit in der Informationstechnik des Bundes abwehren;
- BSIG §3 Absatz 1 Satz 2 Ziffer 2: Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen sammeln und auswerten und die gewonnenen Erkenntnisse anderen Stellen zur Verfügung stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, und Dritten zur Verfügung stellen, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;
- BSIG §3 Absatz 1 Satz 2 Ziffer 4: Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen untersuchen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben;
- BSIG §3 Absatz 1 Satz 2 Ziffer 5: Kriterien, Verfahren und Werkzeuge für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit entwickeln;
- BSIG §3 Absatz 1 Satz 2 Ziffer 8: Sicherheit von informationstechnischen Systemen oder Komponenten prüfen und bewerten sowie Sicherheitszertifikate erteilen;
- BSIG §3 Absatz 1 Satz 2 Ziffer 15: IT-Sicherheitsprodukte und IT-Sicherheitsdienstleistungen für Einrichtungen der Bundesverwaltung bereitstellen;
- BSIG §3 Absatz 1 Satz 2 Ziffer 17: Einrichtungen der Bundesverwaltung in Fragen der Informationssicherheit, einschließlich der Behandlung von Sicherheitsvorfällen, beraten und unterstützen sowie konkrete, praxisnahe Hilfsmittel zur Umsetzung von Informationssicherheitsvorgaben, insbesondere zur Umsetzung der Vorgaben nach den §§ 30 und 44, bereitstellen;

Die Ziele des Projekts kommen explizit diesem Handlungsbedarf nach. Um eine fundierte Einschätzung bezüglich der Fähigkeiten von KI im SSDLC zu erlangen, ist eine Studie über die schon erhältlichen Tools und die Fähigkeiten von KI-Modellen in diesem Gebiet notwendig. Des Weiteren kann auf Grundlage dieser Studie ein breiter Einsatz solcher Tools in der Bundesverwaltung vorbereitet, und der Einfluss auf Bewertungsprozesse, z.B. in der Zertifizierung, wo angenommen werden muss, dass auch bösartige Akteure diese Tools nutzen, ermittelt werden.

1.3 Auftragsgegenstand und Projektziele

Ziel des Projektes ist zunächst, den Stand der Technik im Bereich KI im SSDLC zu eruieren und eine vergleichende Marktübersicht der wichtigsten und leistungsstärksten Codeanalyse- und Hilfstools zu erstellen. Dabei sollen auch Tools berücksichtigt werden, die nicht vollständig auf KI basieren. Aufbauend auf den Ergebnissen dieser Studien soll einerseits der Bewertungsprozess im Rahmen der Softwarezertifizierung des BSIs an die festgestellten Fähigkeiten der Tools angepasst werden, und andererseits eine Referenzarchitektur für OpenCoDE erstellt werden, anhand derer eine Integration ausgewählter Tools in Open CoDE geplant werden kann. Im Einzelnen werden somit folgende Ziele verfolgt:

- 1) Erstellung einer Studie zum Stand der Technik und der Wissenschaft mit Marktübersicht und Analyse vorhandener Tools im SSDLC, mit Fokus auf Tools auf KI-Basis sowie Tools mit KI-Anteil.
 - Erstellung einer Übersicht über verfügbare Tools im SSDLC; hierbei sollen sowohl KI-basierte als auch hybride Ansätze mit KI-Anteil berücksichtigt und mindestens folgende Aspekte betrachtet werden:

-
- Funktionalitäten
 - Interpretierbarkeit des Outputs
 - Benötigtes Expertenwissen
 - Funktionsweise
 - Vertriebsmodelle
 - Open oder Closed Source
 - Einschätzung der Entwicklung auf diesem Feld in der nahen Zukunft (1-2 Jahre)
 - Erarbeitung von Bewertungskriterien, um Tools vergleichbar zu machen und ihre Leistungsfähigkeit einzuschätzen
 - Vergleich der Tools anhand der Bewertungskriterien
 - Begründete Vorauswahl der vielversprechendsten Tools mit Blick auf die folgenden Arbeitspakete und Vorhaben einer Detailbewertung für diese in der Praxis anhand repräsentativer Testfälle
 - Ableiten von Best Practices zur sicheren und zielführenden Nutzung der Tools
 - Zusammenfassung der Ergebnisse und Veröffentlichung in einer BSI-Publikation, die sich an Fachexperten aus dem Bereich von SSDLC und Codeanalyse richtet

2) Untersuchung der Anwendung von KI in der Schwachstellenidentifikation und Aktualisierung der Schwachstellenbewertungskriterien für Common Criteria (AVA-Tabelle) basierend auf empirischen Untersuchungen

- Erstellen von repräsentativen Testfällen, inklusive Durchführung empirischer Untersuchungen
- Aktualisierung der Schwachstellenbewertungskriterien basierend auf den Ergebnissen
- Auswertung der Änderung der Schwachstellenbewertungskriterien
- Empfehlungen für KI-Einsatz hinsichtlich Dual-Use Tools bei Prüfstellen und Herstellern in Form einer Guideline

3) Erarbeitung einer Referenzarchitektur zur Planung der Einführung von KI-Tools des SSDLC in Open CoDE¹

- Erweiterung der vorhandenen Architektur von OpenCoDE
- Begründeter Vorschlag für die Auswahl der KI-Tools inkl. Kostenschätzung
- Schätzung benötigter Hardware inkl. Kostenschätzung
- Konzept zur Umsetzung/Integration in der Open CoDE Umgebung entwickeln und verschriftlichen
- Erarbeitung eines möglichen Betriebsablaufs und Schätzung der Anschaffungs- und Betriebskosten

Die Ergebnisse müssen belastbar und für eine anschließende Vergabe geeignet sein.

¹ www.opencode.de

1.4 Projektstrukturplan

Im Rahmen der Leistungserbringung sind folgende Arbeitspakete (AP) vorgesehen:

- AP 1: Auftaktbesprechung und Feinkonzept (Auftaktbesprechung)
- AP 2: Ermittlung des Forschungs- und Markstandes zum Thema KI im SSDLC, Vergleich der Methoden und Veröffentlichung der Ergebnisse (Studie zu KI im SSDLC)
- AP 3: Erarbeitung von Best Practices zum Einsatz ausgewählter Tools im SSDLC und Erstellung eines Proof of Concepts (Best Practices und PoC)
- AP 4: Zwischenworkshop zur Vorstellung bisheriger Ergebnisse und Feinkonzept (Zwischenworkshop)
- AP 5 (OPTIONAL): Einordnung und Empfehlungen für AVA-Bepunktung in den Common Criteria (Aktualisierung Einordnung CC-Bewertungsmetrik)
- AP 6 (OPTIONAL): Erstellung einer Guideline für den Einsatz von KI-Tools mit Dual-Use in Prüfstellen und ggf. bei Herstellern (Guideline: KI-Tools in der Evaluierung in Prüfstellen)
- AP 7 (OPTIONAL): Erstellung einer Referenzarchitektur für die Integration von KI-Tools des SSDLC in Open CoDE (Referenzarchitektur KI-Tools im SSDLC in Open CoDE)
- AP 8: (OPTIONAL) Abschlusspräsentation der Projektergebnisse und Abschlussbericht (Abschlussworkshop)

AP 5, 6, 7 und 8 sind optionale Leistungen. Diese müssen vom Bieter angeboten werden, der AG verzichtet jedoch ggf. generell auf deren Beauftragung. Die Entscheidung wird durch den AG anhand der Zwischenergebnisse getroffen.

Die Beauftragung von AP 5 und 7 ist dabei abhängig von den Ergebnissen aus AP 2 und 3. Zeigen die Ergebnisse aus AP 2 keine nennenswerten Fähigkeiten oder Tools auf, erscheinen die Tools auch bei Befolgung der Best Practices aus AP 3 für einen sicheren und effizienten Einsatz im SSDLC ungeeignet oder wird der PoC aus AP 3 den zuvor im Anforderungskatalog definierten Anforderungen nicht gerecht, ist eine Weiterverwendung der Ergebnisse in AP 5 und AP 7 nicht sinnvoll und das Projekt wird nicht fortgeführt.

Sollte keines der AP 5, 6 und 7 durchgeführt werden, wird auch AP 8 nicht beauftragt, da sämtliche Ergebnisse bereits im Zwischenworkshop (AP 4) vorgestellt wurden.

Ein Anspruch auf Beauftragung der optionalen Arbeitspakete besteht nicht.

2 Beschreibung der Arbeitspakete

Der Auftragnehmer (AN) hat die in den folgenden Arbeitspaketen dargestellten Leistungen zu erbringen.

2.1 Arbeitspaket 1: Auftaktbesprechung und Feinkonzept (Auftaktbesprechung)

Zu Beginn des Projekts findet eine virtuelle Auftaktbesprechung zwischen AG und allen wesentlich am Projekt beteiligten Mitgliedern des Projektteams des AN statt. Die Auftaktbesprechung ist durch den AN nach Absprache mit dem AG in einem geeigneten Format zu organisieren. Es wird vorausgesetzt, dass sich die Teilnehmer vor der Besprechung umfassend mit dem Projekt auseinandergesetzt haben. Die Dauer sollte einen halben Arbeitstag nicht überschreiten. Von Seiten des AN sollten maximal 4 Personen teilnehmen.

In der Auftaktbesprechung wird vom AN das Vorgehen zu allen Arbeitspaketen im Detail vorgestellt. Verbleibende offene Fragen werden zwischen AG und AN diskutiert und verbindlich geklärt. Die Planung wird gegebenenfalls weiter konkretisiert und die Regeln der Zusammenarbeit verabschiedet. Hierbei liegt der Fokus auf AP 2, AP 3 und AP 4.

Ferner sind die generellen Kommunikationswege zu etablieren und die Erreichbarkeit der beteiligten Personen seitens AN und AG abzustimmen. Auch werden die Wege zur Übermittlung und Abstimmung von Projekthinhalten, also von Dokumenten und sonstigen Leistungsgegenständen, abgesprochen.

Der AN erstellt ein Besprechungsprotokoll und legt dieses dem AG innerhalb von einer Woche nach der Besprechung vor. Kam es bei der Auftragserteilung zu zeitlichen Verschiebungen (vgl. Kapitel 6.2.1.4, Zuschlagskriterium „Zahlungs- und Meilensteinplan“) so werden die daraus ggf. resultierenden Terminverschiebungen verbindlich zwischen AN und AG abgestimmt. Der aktualisierte Zahlungs- und Meilensteinplan ist vom AN mit dem Besprechungsprotokoll vorzulegen.

2.2 Arbeitspaket 2: Ermittlung des Forschungs- und Markstandes zum Thema KI im SSDLC, Vergleich der Methoden und Veröffentlichung der Ergebnisse (Studie zu KI im SSDLC)

Der AN erstellt in diesem Arbeitspaket eine umfassende Studie zum aktuellen Stand der Technik im Bereich KI im SSDLC. Die Studie soll als Grundlage für die folgenden Arbeitspakete dienen, deshalb müssen die Inhalte mit Blick auf die Weiterverarbeitung erstellt werden. Der AN stimmt sich hierzu regelmäßig und anlassbezogen eng mit dem AG ab.

Im Einzelnen müssen mindestens folgende Punkte im Rahmen der Studie bearbeitet werden:

1. Der AN erstellt eine **Übersicht** über die am Markt erhältlichen Tools (einzelne Produkte) und Toolklassen (Kategorie, Sammlung von Tools mit derselben Zielsetzung) sowie über den aktuellen Forschungsstand zum Einsatz von KI im SSDLC. Es sollen hierbei auch hybride Ansätze betrachtet werden. Dabei muss auf diverse Aspekte der Tools und Toolklassen eingegangen werden; insbesondere sollen folgende Fragen beantwortet werden:
 - Welche Funktionalitäten hat das Tool? Welche Programmiersprachen werden unterstützt?
 - Inwiefern lassen sich die Ausgaben des Tools nachvollziehen? Welches Maß an Expertise ist erforderlich?
 - Welches Vertriebsmodell wird genutzt?
 - Ist das Tool Open Source?
 - Wie nutzt das Tool KI? Welche Modelle werden zu welchen Zwecken verwendet?

-
- Welche Stärken und Schwächen weist das Tool auf?
 - Wie unterscheidet sich das Tool von anderen Tools derselben Toolklasse?
 - Welche Schnittstellen zu anderen Tools hat es? Ist es auf bestimmte Dateiformate angewiesen?
 - Welche Basisfunktionen sollte eine Toolklasse in einem gewissen Anwendungsgebiet (z.B. Schwachstellenidentifikation, Schwachstellenbehebung, automatisiertes Vexing, ...) erfüllen?
2. Um die Tools aus der Übersicht vergleichbar zu machen, müssen vom AN nachvollziehbare und aussagekräftige **Bewertungskriterien** und entsprechende Gewichtungen erarbeitet und mit dem AG abgestimmt werden. Die Bewertungskriterien sollen falls möglich ganze Toolklassen abdecken und vergleichbar machen. Im Anschluss führt der AN eine Multi-Criteria-Analyse (MCA) durch, um die Tools zu vergleichen, Stärken und Schwächen aufzuzeigen, sowie Herausstellungsmerkmale zu benennen. Die Verschriftlichung der MCA kann in tabellarischer Form erfolgen; das genaue Format stimmt der AN im Voraus mit dem AG ab. Das Ergebnis der Analyse muss eine begründete, nachvollziehbare Vorauswahl der vielversprechendsten Ansätze sein (pro Toolklasse max. 3, Abweichungen in Abstimmung zwischen AG und AN möglich). Die Auswahl erfolgt in enger Abstimmung mit dem AG. Die Anzahl der gewählten Tools darf ein kritisches Maß nicht übersteigen, sodass eine Bearbeitung in der vorgesehen Anzahl an Personentagen möglich ist (vgl. Kapitel 3)
 3. Auf Grundlage der Vergleiche sind die zuvor ausgewählten Tools im Detail zu untersuchen. Dazu müssen einerseits geeignete und repräsentative Testfälle geschaffen werden und andererseits passende Metriken definiert werden, um die Leistungsfähigkeit in der Praxis bewerten zu können. Auf Basis dieser Testfälle werden die vorausgewählten Tools praktisch untersucht und unter Berücksichtigung der Metriken miteinander verglichen. Dabei muss auf die unterschiedlichen Toolklassen eingegangen werden. Eine separate Betrachtung für die verschiedenen Anwendungsgebiete muss, falls nötig, vorgenommen werden. Im Zuge dieser Auswertung stehen, falls nötig, Gelder für Softwarelizenzen zum Abruf bereit (vgl. Kapitel 3). Geplante Ausgaben des AN werden vorab mit dem AG abgestimmt und erfordern dessen Zustimmung.
 4. Unter Berücksichtigung beider Vergleiche, die also einerseits auf der MCA basieren (siehe oben, 2.) und andererseits die praktischen Untersuchungen anhand von Testfällen nutzen (siehe oben, 3.), erfolgt eine Einschätzung, welche der Ansätze am vielversprechendsten erscheinen und im weiteren Verlauf des Projekts mindestens betrachtet werden müssen

Der AN muss die Ergebnisse seiner Untersuchungen aus 1., 2. und 3. in verständlicher Form vollständig und strukturiert in einem zur Veröffentlichung geeigneten, Dokument zusammenfassen, das sich an Fachexperten aus der KI-Forschung und der Wirtschaft richten soll. Das Dokument muss in zwei Versionen, einmal in deutscher und einmal in englischer Sprache erstellt werden. In das Dokument müssen also, wie in den Teilaufgaben bereits beschrieben, sowohl die Übersicht zu bestehenden Ansätzen, als auch die gewichteten Bewertungskriterien und der auf ihnen basierende Vergleich (MCA), eine Beschreibung der Testfälle und Metriken und der auf ihnen basierende Vergleich sowie die begründete Auswahl vielversprechender Ansätze einfließen. Aus Gründen der Produktneutralität müssen die Informationen zu konkreten, bestehenden Softwareprodukten im durch den AN zu erstellenden Dokument von den übrigen Informationen separiert werden, beispielsweise durch Einfügen eines eigenen produktbezogenen Kapitels. Des Weiteren muss auf die Dual-Use-Problematik eingegangen werden, und das Dokument so gestaltet werden, dass eine missbräuchliche Verwendung der Ergebnisse möglichst vermieden wird.

Der Umfang des Berichts muss 30 – 45 mit Inhalt gefüllte Seiten in der Schriftart „BundesSans Regular“ mit Schriftgröße 11 und üblichem Zeilenabstand umfassen; auf die Teilaufgaben 2 und 3 müssen hierbei mindestens die Hälfte der Länge des Dokuments entfallen, sodass sichergestellt ist, dass diese Themen ausreichend beleuchtet wurden. Das Ergebnisdokument ist auf Grundlage des zum Zeitpunkt der Erstellung aktuellen Standes von Wissenschaft und Technik zu erstellen. Die Erarbeitung hat unter Anwendung anerkannter wissenschaftlicher Methoden sowie unter Beachtung der Grundsätze guter wissenschaftlicher Praxis zu erfolgen. Abweichungen von diesen Vorgaben sind nur nach Absprache mit dem AG möglich.

Jedweder Einsatz von KI zur Erstellung des Dokuments ist nur nach vorheriger Absprache zwischen AN und AG und mit Zustimmung des AG möglich.

Das Ergebnisdokument wird dem AG zum Abschluss des AP durch den AN zusammenfassend in einem virtuellen Termin vorgestellt und durch den AG abgenommen.

Die Ergebnisse von 4. sind nicht Teil der Veröffentlichung, müssen aber dennoch schriftlich dokumentiert und dem AG am Ende des APs in verständlicher Form übermittelt werden. Das genaue Format wird im Rahmen des Auftaktworkshops abgestimmt.

Für AP 2 wird durch den AG eine Obergrenze von 130 PT festgelegt. Die Vorgaben hinsichtlich ggf. anfallender Lizenzkosten sind durch den AN zu beachten (vgl. Kapitel 3.1.2.2). Um den Stand der Arbeiten zu verfolgen und dem AG die Möglichkeit zu geben, inhaltliche Schwerpunkte zu setzen und Feedback zu geben, finden regelmäßig alle zwei Wochen sowie bei Bedarf anlassbezogene Besprechungen über Videokonferenz zwischen AG und AN statt (jeweils max. 2 Stunden). Der AN berichtet hierbei über den aktuellen Stand der Arbeiten und die geplanten inhaltlichen Aktivitäten der nächsten zwei Wochen. Er fertigt zu jeder solchen Besprechung ein kurzes Ergebnisprotokoll an und legt dieses dem AG innerhalb von drei Werktagen nach der jeweiligen Besprechung zur Abnahme vor.

Falls der AG feststellt, dass, auf Basis der Ergebnisse von AP 2 die Projektziele wahrscheinlich nicht oder nur unzureichend erfüllt werden können, hat er die Möglichkeit eine Nachbesserung durch den AN zu fordern oder das Projekt an dieser Stelle vorzeitig zu beenden. Die Wahrnehmung dieser Optionen wird durch den AG sachlich begründet und erfolgt innerhalb von zwei Wochen nach dem Vorstellungstermin für das Ergebnisdokument und dem Vorliegen der schriftlichen Ergebnisse. Um einen solchen Abbruch nach Möglichkeit zu vermeiden, gibt der AG regelmäßiges Feedback.

2.3 Arbeitspaket 3: Erarbeitung von Best Practices zum Einsatz ausgewählter Tools im SSDLC und Erstellung eines Proof of Concepts (Best Practices und PoC)

In diesem Arbeitspaket muss der AN basierend auf den bisherigen Untersuchungen Best Practices zum Einsatz der in AP 2 untersuchten Tools herleiten. Die Best Practices sollen den Einsatz der Tools sicher und effizient machen, und auf die größten Probleme der Tools eingehen. Idealerweise sind die Best Practices auf alle Tools einer Toolklasse anwendbar, können falls nötig aber auch spezifischer sein. Einhergehend mit der Erarbeitung dieser Best Practices ist ein PoC zu entwickeln, welcher die Best Practices für die ausgewählten Tools entsprechend umsetzt und aufzeigt, dass der Einsatz unter den Vorgaben der Best Practices möglich und praktikabel ist. Der PoC ist somit als Framework aufzusetzen, das den Best Practices folgt und die gewählten Tools im Rahmen dieser Best Practices nutzbar macht. Die genaue Form des PoC ist im Laufe von AP 2 und 3 mit dem AG abzustimmen, und ist abhängig von den Ergebnissen der Untersuchungen. Dies soll als Grundlage zur Weiterarbeit im Rahmen folgender APs dienen.

Die Best Practices können mitunter auf die korrekte Verwendung der Tools (z.B. Besonderheiten bei der Nutzung) abzielen oder sich auf den Umgang mit ihren Ausgaben (z.B. im Hinblick auf False Positives) beziehen. Sie sind in Form von konkreten, in der Praxis anwendbaren Leitlinien darzustellen, und müssen ausreichend begründet werden. Dabei müssen die entsprechenden Toolklassen berücksichtigt und die Best Practices entsprechend den speziellen Anforderungen angepasst werden.

Der AN muss die Best Practices in einer für Anwender verständlichen und praxisorientierten Form in einem Dokument festhalten. Dieses muss zwischen 5 und 15 mit Inhalt gefüllte Seiten in der Schriftart „BundesSans Regular“ mit Schriftgröße 11 und üblichem Zeilenabstand umfassen. Abweichungen hiervon müssen mit dem AG abgestimmt werden. Das Dokument soll, ggf. gemeinsam mit dem PoC (siehe unten), veröffentlicht werden.

Für den PoC ist vom AN zunächst ein Anforderungskatalog zu definieren, welcher mit dem AG abgestimmt werden muss. Der Anforderungskatalog ist in Tabellenform zu erstellen und muss sich auf die wesentlichen Punkte beschränken (ca. 1 DIN-A4 Seite). Er soll Missverständnissen in der Erwartungshaltung für beide Seiten vorbeugen und sicherstellen, dass der PoC zur Durchführung weiterer Arbeitsschritte (AP 5, 6, 7) geeignet ist. Erst nach der Freigabe des Anforderungskatalogs kann mit der Implementierung des PoCs begonnen werden.

Die Entwicklung des PoC ist umfassend zu dokumentieren und Entscheidungen schriftlich zu begründen. Bei der Erstellung ist darauf zu achten, dass die notwendigen Voraussetzungen auch im behördlichen Umfeld vorhanden sind (z.B. benötigte Hardware oder Zugang zu Onlinediensten), und die Best Practices sowohl in der Wirtschaft als auch in Behörden umsetzbar sind. Wenn alternative Lösungen möglich sind, sind diese zu erwähnen und theoretisch darzustellen.

Die Ergebnisse dieses AP sollen als Anhang an den Bericht angefügt werden, der in AP 2 erstellt wird. Ob der Anhang Teil der Veröffentlichung wird, wird in Absprache zwischen AN und AG nach Sichtung der Ergebnisse entschieden.

Für AP 3 wird durch den AG eine Obergrenze von 50 PT festgelegt. Um den Stand der Arbeiten zu verfolgen und dem AG die Möglichkeit zu geben, inhaltliche Schwerpunkte zu setzen und Feedback zu geben, finden regelmäßig alle zwei Wochen sowie bei Bedarf anlassbezogene Besprechungen über Videokonferenz zwischen AG und AN statt (jeweils max. 2 Stunden). Der AN berichtet hierbei über den aktuellen Stand der Arbeiten und die geplanten inhaltlichen Aktivitäten der nächsten zwei Wochen. Er fertigt zu jeder solchen Besprechung ein kurzes Ergebnisprotokoll an und legt dieses dem AG innerhalb von drei Werktagen nach der jeweiligen Besprechung zur Abnahme vor.

2.4 Arbeitspaket 4: Zwischenworkshop zur Vorstellung bisheriger Ergebnisse und Feinkonzept (Zwischenworkshop)

In diesem AP muss der AN dem AG die Ergebnisse aus AP 2 (Studie zu KI im SSDLC) und AP 3 (Best Practices und PoC) umfassend als PowerPoint-Präsentation darstellen. Die bis zu diesem Zeitpunkt durchgeführten Schritte sind zu beschreiben sowie die Resultate und Schlussfolgerungen aufzuzeigen. Auch wird das weitere Vorgehen in Bezug auf AP 5, 6, 7 und 8 abgestimmt und verbleibende offene Fragen zwischen AG und AN diskutiert und verbindlich geklärt.

Die Zwischenpräsentation ist durch den AN in Absprache mit dem AG in einem geeigneten virtuellen Format (z.B. Video- oder Telefonkonferenz) zu organisieren. Die Präsentationsfolien werden dem AG fünf Werktage vor der Präsentation durch den AN zur Verfügung gestellt und dürfen vom AG für weitere interne und externe Präsentationen verwendet werden. Die Präsentation wird auf 4 Stunden begrenzt.

Der AN erstellt ein Besprechungsprotokoll und legt dieses dem AG innerhalb von einer Woche nach der Besprechung vor.

2.5 Arbeitspaket 5 (OPTIONAL): Einordnung und Empfehlungen für AVA-Bepunktung in den Common Criteria (Aktualisierung Einordnung CC-Bewertungsmetrik)

(EU)CC-Evaluierungen erfolgen nach dem jeweils aktuellen Stand der Technik und der Wissenschaft. Dementsprechend müssen Prüfstellen, Hersteller und Zertifizierungsstellen technische Entwicklungen generell beim Testen von Softwareprodukten und insbesondere auch bei der Schwachstellenanalyse berücksichtigen. Der Fokus dieses APs liegt im Bereich von Softwareschwachstellen, insbesondere nicht im Bereich der Kryptoseitenkanalanalyse.

Durch KI-Tools und -Techniken könnten sich insbesondere Angriffe vereinfachen, die entweder neue Angriffspfade ermöglichen oder bisher entweder nur mit großem Zeitaufwand und/oder nur mit umfassenden, technischen Fachkenntnissen (Experten) durchgeführt werden konnten, siehe hierzu CEM:2022, Anhang B 6.2.3. Sofern sich hier neue Möglichkeiten ergeben und/oder sich Aufwände reduzieren, hat dies erhebliche Auswirkungen auf die Sicherheit von IT-Produkten. CEM:2022², Anhang B 6.2.3 unterscheidet hier nach

“The following factors should be considered during analysis of the attack potential required to exploit a vulnerability:

a) Time taken to identify and exploit (Elapsed Time);

b) Specialist technical expertise required (Specialist Expertise); [Welche Fachkenntnisse sind erforderlich um einen Angriff überhaupt durchführen zu können.]

c) Knowledge of the TOE design and operation (Knowledge of the TOE); [Im Softwareumfeld ist häufig davon auszugehen, dass der Code selbst nicht geschützt oder/und frei verfügbar ist.]

d) Window of opportunity; [Zugriffsmöglichkeit auf den Evaluierungsgegenstand respektive das IT-Produkt. Hier ist beispielsweise zu berücksichtigen, wie lange ein Zugriff möglich/notwendig ist, ohne dass ein solcher auffällt und (automatische oder manuelle) Gegenmaßnahmen ergriffen werden.]

e) IT hardware/software or other equipment required for exploitation”

Von besonderem Interesse für AP 5 sind demnach KI-Tools und -Techniken, die ein oder mehrere der o.g. Elemente der Angriffs-Bewertungsmetrik gegenüber klassischen Angriffs- (Brute Force, Injection, Speicherüberläufe etc.) und Analysetechniken (statischer/dynamischer Codeanalyse, Fuzzing etc.) signifikant reduzieren bzw. vereinfachen.

Im Rahmen dieses AP wird untersucht, inwiefern die Schwachstellenbewertungskriterien in der Common Criteria Zertifizierung an die eventuell neuen Gegebenheiten, die durch den (böswilligen) Einsatz von KI in der Schwachstellensuche und -ausnutzung entstehen, angepasst werden müssen. Dabei erfolgt unter Verwendung der Ergebnisse von AP 2 und AP 3 eine Einordnung der in AP 2 und AP 3 identifizierten Fähigkeiten der KI-Tools in die AVA-Bepunktungstabelle entsprechend oben genannter Vorgaben aus der CEM durch den AN in Zusammenarbeit mit dem AG. So ist beispielsweise denkbar, dass mithilfe von KI z.B. generell kürzere ‚windows of opportunity‘ oder geringere ‚Specialist Expertise‘ nötig sind, um Schwachstellen zu identifizieren und auszunutzen. Der AN muss hierzu die Ergebnisse aus AP 2 und 3 so aufbereiten, dass sie in diesem AP nutzbar sind, mit einem Fokus auf Dual-Use Tools. Insbesondere die Testfälle müssen mit Hinblick auf die Schwachstellenbewertungskriterien ausgewertet und bei Bedarf ergänzt werden. Hierfür sollen auch empirische Untersuchungen durchgeführt werden. Falls nötig, müssen die Ergebnisse aus AP 2 und 3 noch einmal mit Hinblick auf die Anforderungen dieses AP vertieft werden.

Auf Basis der Untersuchungen werden konkrete, schriftliche Empfehlungen und Erläuterungen für die Bepunktung von Schwachstellen anhand der AVA-Bepunktungstabelle, die sich aus dem (böswilligen) Einsatz von KI in der Schwachstellensuche ergeben, erarbeitet. Darin erfolgt insbesondere ein Vergleich zwischen der Bepunktung von Schwachstellen anhand der AVA-Bepunktungstabelle einmal ohne den Einsatz von KI und einmal mit dem Einsatz von KI. Alle Änderungen und Entscheidungen werden dabei schriftlich begründet.

Aufgrund des erforderlichen Expertenwissens im Bereich der CC-Zertifizierung unterstützt und berät der AG den AN bei Bedarf. Grundsätzlich wird jedoch vorausgesetzt, dass sich alle Beteiligten im Vorfeld mit CEM:2022, Anhang B auseinandergesetzt haben.

Für AP 5 wird durch den AG eine Obergrenze von 66 PT festgelegt. Um den Stand der Arbeiten zu verfolgen und dem AG die Möglichkeit zu geben, inhaltliche Schwerpunkte zu setzen und Feedback zu geben, finden regelmäßig alle zwei Wochen sowie bei Bedarf anlassbezogene Besprechungen über Videokonferenz zwischen AG und AN statt (jeweils max. 2 Stunden). Der AN berichtet hierbei über den aktuellen Stand der

² <https://www.commoncriteriaportal.org/cc/index.cfm>

Arbeiten und die geplanten inhaltlichen Aktivitäten der nächsten zwei Wochen. Er fertigt zu jeder Besprechung ein Ergebnisprotokoll an und legt dieses dem AG innerhalb von drei Werktagen nach der jeweiligen Besprechung zur Abnahme vor.

2.6 Arbeitspaket 6 (OPTIONAL): Erstellung einer Guideline für den Einsatz von KI-Tools mit Dual-Use in Prüfstellen und ggf. bei Herstellern (Guideline: KI-Tools in der Evaluierung in Prüfstellen)

(EU)CC-Evaluierungen erfolgen nach dem jeweils aktuellen Stand der Technik und der Wissenschaft. Dementsprechend müssen Prüfstellen, Hersteller und Zertifizierungsstellen technische Entwicklungen generell beim Testen von Softwareprodukten und insbesondere auch bei der Schwachstellenanalyse berücksichtigen. Dieses AP dient dazu, dass sich die genannten Gruppen frühzeitig auf diesbezügliche technische Entwicklungen im Bereich KI vorbereiten und, sofern vorhanden, entsprechende Tools nutzen können. Der Fokus dieses APs liegt im Bereich von Softwareschwachstellen, insbesondere nicht im Bereich der Kryptoseitenkanalanalyse.

Im Rahmen der Common Criteria Zertifizierung werden die Prüfungen von durch das BSI anerkannten Prüfstellen durchgeführt. Werden im Rahmen von AP 5 die Empfehlungen für die AVA-Bepunktung angepasst, so müssen diese Prüfstellen und ggf. die Hersteller in die Lage versetzt werden, diese Empfehlungen umzusetzen. Der Einsatz der KI-Tools, welche die Empfehlungen aus AP 5 begründen, ist hierbei wichtig.

In diesem AP ist unter Berücksichtigung des aktuellen Forschungsstands eine Guideline zu erstellen, die den Einsatz von KI-basierten Tools in den Prüfstellen vorbereitet und als Zeithorizont insbesondere die nächsten 2 bis 3 Jahre abdeckt. Der AN muss sich dementsprechend intensiv mit kürzlichen, aktuellen sowie erwartbaren Entwicklungen im Kontext des Testens von Softwareprodukten und der Schwachstellenanalyse mittels KI auseinandersetzen. Die Guideline sollte auch für Hersteller von IT-Sicherheitssoftware verständlich sein, damit diese die entsprechenden Tests und Analysen grundsätzlich nachvollziehen können. Dabei ist mindestens auf folgende Punkte im Detail einzugehen:

- Die Ergebnisse aus AP 5 müssen Teil der Guideline sein.
- Welche Toolklassen sind grundsätzlich relevant?
- Welche KI-Tools und -Techniken sind oder könnten zukünftig absehbar geeignet (sein), um in Prüfstellen genutzt zu werden?
- Welche KI-Tools und -Techniken sollten Prüfstellen und Hersteller „im Auge behalten“, um nicht absehbar von KI-Entwicklungen im Sinne dieses AP überrascht zu werden?
- Welche Kosten und Voraussetzungen sind mit der Einführung entsprechender Tools verbunden?
- Was ist bei der Nutzung der KI-Tools und -Techniken zu beachten?
- Für welche Schwachstellenkategorien (z. B. OWASP) ist das jeweilige Tool bzw. die jeweilige Technik geeignet?

Hinweis: Hier kann es Überschneidungen zu den Ergebnissen von AP 7 geben, insb. in Hinsicht auf Anwendung von KI-Tools in der sicheren Softwareentwicklung. Ein Abgleich muss hier stattfinden.

Das Vorgehen muss dabei stets dokumentiert werden, und Entscheidungen schriftlich begründet werden. Für AP 6 wird durch den AG eine Obergrenze von 60 PT festgelegt. Um den Stand der Arbeiten zu verfolgen und dem AG die Möglichkeit zu geben, inhaltliche Schwerpunkte zu setzen und Feedback zu geben, finden regelmäßig alle zwei Wochen sowie bei Bedarf anlassbezogene Besprechungen über Videokonferenz

zwischen AG und AN statt (jeweils max. 2 Stunden). Der AN berichtet hierbei über den aktuellen Stand der Arbeiten und die geplanten inhaltlichen Aktivitäten der nächsten zwei Wochen. Er fertigt zu jeder Besprechung ein kurzes Ergebnisprotokoll an und legt dieses dem AG innerhalb von drei Werktagen nach der jeweiligen Besprechung zur Abnahme vor.

2.7 Arbeitspaket 7 (OPTIONAL): Erstellung einer Referenzarchitektur für die Integration von KI-Tools des SSDLC in Open CoDE (Referenzarchitektur KI-Tools im SSDLC in Open CoDE)

Open CoDE³ ist die gemeinsame Plattform der öffentlichen Verwaltung zum Austausch von Open Source Software (<https://opencode.de/de>). Projekte auf dieser Plattform abzusichern führt dementsprechend zu einer Erhöhung der Cybersicherheit in der Bundesverwaltung insgesamt. OpenCoDE stellt bereits diverse Tools zur Verbesserung der Sicherheit des hinterlegten Codes zur Verfügung. Dieser Katalog soll durch die Einführung von KI-Tools erweitert werden, die den SSDLC unterstützen. Durch den konsequenten Einsatz von Open Source besteht die Chance, mit den eingesetzten Mitteln eine große Wirkung zu erzielen und den State of the Art voranzutreiben. Bei den eingesetzten KI-Modellen ist aus Gründen der digitalen Souveränität der Einsatz von Open Weight Modellen wünschenswert, auch wenn bei der Erstellung von Open Source Software die Datensouveränität nicht unbedingt im Fokus steht. Auch das Finetuning von Open Weight Modellen für optimierte Ergebnisse beim gewünschten Einsatzzweck sollte Berücksichtigung finden.

Dafür muss in diesem AP eine Referenzarchitektur erstellt werden, die die Integration der KI-Tools im SSDLC in OpenCoDE darstellt. Dies umfasst mindestens:

- Auflistung und Abwägung der Vor- und Nachteile verschiedener Tools, mit Bezug zu den speziellen Gegebenheiten in OpenCoDE
- Vorauswahl geeigneter Tools für den Einsatz in OpenCoDE mit Begründung
- Erstellung mindestens einer Referenzarchitektur, die die mögliche Integration der Tools in OpenCoDE darstellt
- Möglichst genaue und fundierte Schätzung der anfallenden einmaligen und wiederkehrenden Kosten in Anschaffung und Betrieb. Dies beinhaltet auch die Schaffung der nötigen technischen Rahmenbedingungen.

Für OpenCoDE sind hierbei primär Tools von Interesse, die im Secure Software Development Life Cycle zu späteren Phasen, i.e. Testing und Deployment, eingesetzt werden. Darunter fallen beispielsweise:

- Beim Fuzzing kann KI die Logik der Anwendung berücksichtigen und dadurch besonders effektiv Edge Cases finden. Diese ermittelten Edge Cases finden auch bei der Testfallgenerierung Verwendung.
- Wünschenswert ist eine auf Grundlage von Tickets automatisierte Generierung von Testfällen. Diese stellen dann einen Teil des Fixes dar und sorgen für Qualität durch eine Ergänzung der Testabdeckung und schützen vor Regressionen.
- In der Deployment-Phase erkennt KI auffällige Telemetriedaten und kann darauf basierend Rollbacks auslösen, entweder halbautomatisch mit menschlicher Bestätigung oder vollautomatisch.
- Automatische Vulnerability Triage: Hierbei werden Ergebnisse aus statischen und dynamischen Analysen korreliert und mit einer Reachability-Analyse verknüpft, um die Relevanz von gemeldeten Schwachstellen zu bewerten. Auch automatisches VEXing ist vorstellbar.

³ <https://opencode.de/de>

-
- Entdeckt die KI eine neue Schwachstelle in einer Bibliothek, scannt sie proaktiv alle Produktionsumgebungen, ermittelt das Risiko und erstellt einen virtuellen Patch entweder in der Web Application Firewall oder in einem Sidecar-Proxy-Container (Stichwort Self-healing Architecture).
 - KI kann schließlich auch Natural Language Policy Enforcement ermöglichen, also die Durchsetzung von Sicherheitsrichtlinien durch Anweisungen in natürlicher Sprache.

Auf Grundlage der Referenzarchitektur erstellt ZenDiS eine Roadmap. Dies ist bei der Bearbeitung dieses AP in allen Schritten zu beachten.

Hinweis: Hier kann es Überschneidungen zu den Ergebnissen von AP 6 geben, insb. in Hinsicht auf Anwendung von KI-Tools in der sicheren Softwareentwicklung. Ein Abgleich muss hier stattfinden.

Die Referenzarchitektur ist schriftlich auszuarbeiten, zu begründen und zusammen mit den Erläuterungen bezüglich geeigneter Tools auf mindestens 5 mit Inhalt gefüllte Seiten in der Schriftart „BundesSans Regular“ mit Schriftgröße 11 und üblichem Zeilenabstand festzuhalten.

Für AP 7 wird durch den AG eine Obergrenze von 50 PT festgelegt. Um den Stand der Arbeiten zu verfolgen und dem AG die Möglichkeit zu geben, inhaltliche Schwerpunkte zu setzen und Feedback zu geben, finden regelmäßig alle zwei Wochen sowie bei Bedarf anlassbezogene Besprechungen über Videokonferenz zwischen AG und AN statt (jeweils max. 2 Stunden). Der AN berichtet hierbei über den aktuellen Stand der Arbeiten und die geplanten inhaltlichen Aktivitäten der nächsten zwei Wochen. Er fertigt zu jeder solchen Besprechung ein kurzes Ergebnisprotokoll an und legt dieses dem AG innerhalb von drei Werktagen nach der jeweiligen Besprechung zur Abnahme vor.

2.8 Arbeitspaket 8 (OPTIONAL): Abschlusspräsentation der Projektergebnisse und Abschlussbericht (Abschlussworkshop)

Die Projektergebnisse werden im Rahmen einer (maximal) halbtägigen Abschlussveranstaltung vom AN vor Fachpublikum (u.a. BSI-Mitarbeitende) präsentiert. Die Veranstaltung ist inhaltlich und organisatorisch grundsätzlich vom AN zu planen. Die Besprechung findet im BSI als virtuelle Besprechung mit Einwahlmöglichkeit für Mitarbeitende des BSI statt. Die Details der Durchführung der Veranstaltung werden im Vorfeld vom BSI festgelegt bzw. zwischen dem BSI und dem AN abgestimmt. Bei der Präsentation werden die wesentlichen Erkenntnisse des Projektes vorgestellt. Dies schließt u. a. folgende Punkte ein:

- Aus AP 2 werden die untersuchten KI-Tools im SSDLC zusammenfassend präsentiert und wesentliche Ergebnisse der Studie vorgestellt.
- Die in AP 3 erarbeiteten Best Practices und der erstellte PoC wird kurz vorgestellt.
- Wurden optionale APs bearbeitet, sind die jeweiligen Ergebnisse ausführlich zu präsentieren:
 - Zu AP 5 sind die Änderungen in der Common Criteria Bewertungsmetrik im Bereich AVA vorzustellen, zusammen mit den Gründen für die jeweiligen Anpassungen.
 - Zu AP 6 ist die Guideline zu präsentieren, die aufzeigt, wie KI-Tools zur Schwachstellenanalyse in Prüfstellen und ggf. bei Herstellern eingesetzt werden können und welche Tools wofür geeignet sind.
 - Zu AP 7 ist die Referenzarchitektur vorzustellen und zu erläutern, wieso diese Architektur gewählt wurde und welche Tools geeignet sind.
- Etwaige offene Fragen und mögliche Weiterentwicklungen/nächste Schritte sind vom AN im Anschluss zu benennen.

Die Präsentationsunterlagen (Foliensatz in MS PowerPoint) stellt der AN dem BSI mindestens zehn Werktage vor der Präsentation zur Freigabe zur Verfügung. Von Seiten des BSI können weitere Teilnehmer dazu eingeladen werden. Die teilnehmenden Personen des AN müssen in der Lage sein, Detailfragen zu den

Inhalten von anwesenden Experten beantworten zu können. Die Anzahl der teilnehmenden Personen seitens des AN ist auf maximal fünf Personen zu beschränken. Die Videokonferenz ist vom AN zu organisieren.

Zudem erstellt der AN einen Abschlussbericht, der ebenfalls auf die o.g. Punkte zusammenfassend eingeht. Dieser muss, etwaige Anhänge ausgerechnet, etwa fünf mit Inhalt gefüllte Seiten in der Schriftart „BundesSans Regular“ mit Schriftgröße 11 und üblichem Zeilenabstand umfassen. Abweichungen hiervon müssen mit dem AG abgestimmt werden.

3 Zahlungs- und Meilensteinplan, Projektplan und Vergütung

Die nachfolgenden Kapitel geben einen Überblick über die Vergütung und den zeitlichen Projektverlauf.

3.1 Vergütung

Die Vergütung erfolgt abhängig von den einzelnen Arbeitspaketen / der Art der Leistung entweder als Festpreis oder nach Aufwand bis zu einer maximalen Obergrenze (siehe die verbindlichen Vorgaben in Kapitel 3.2, Tabelle 1, Spalte „Art der Vergütung“).

3.1.1 Vergütung von AP nach Festpreis

Die Vergütungen der Arbeitspakete 1 und 4 sowie des optionalen Arbeitspakets 8 erfolgen per Festpreis.

3.1.2 Vergütung von AP nach Aufwand

Die Arbeitspakete 2 und 3 sowie der optionalen Arbeitspakete 5, 6 und 7 werden nach Aufwand bis zu einer maximalen Obergrenze vergütet. Hierzu sind die tatsächlich angefallenen Aufwände bei Rechnungsstellung zu belegen. Angefallene Aufwände, die nicht zuvor mit dem Auftraggeber abgestimmt wurden, können nicht vergütet werden.

3.1.2.1 Personalkosten

Der Auftraggeber legt für die Arbeitspakete 2 und 3 sowie der optionalen Arbeitspakete 5, 6 und 7 ein jeweiliges Abrufkontingent in Form von Personentagen fest:

- AP 2: 130 Personentage
- AP 3: 50 Personentage
- Opt. AP 5: 66 Personentage
- Opt. AP 6: 60 Personentage
- Opt. AP 7: 50 Personentage

Die maximale Obergrenze ergibt sich bei diesen Arbeitspaketen somit aus der vorgegebenen Kontingentgröße und den im Angebot anzugebenden Tagessätzen (siehe Kapitel 6.2.1.4, Zuschlagskriterium 2.3 „Kalkulation der maximalen Obergrenzen“).

Gemeinkosten, Reisekosten sowie sonstige Kosten werden, sofern nicht in Kapitel 3.1.2.2 aufgeführt, nicht gesondert vergütet und müssen daher bereits in den veranschlagten Tagessätzen enthalten sein.

Die angegebenen Tagessätze basieren auf acht Zeitstunden.

Die angefallenen personellen Aufwände sind viertelstundengenau in Rechnung zu stellen und mittels eines Leistungsnachweises (Muster siehe Kapitel D) zu belegen. Der Leistungsnachweis enthält mindestens Angaben zum Leistungsdatum, zu den jeweils eingesetzten Mitarbeitenden, zum zugehörigen Arbeitspaket und zu den jeweils erbrachten Zeiten sowie eine Kurzbeschreibung der jeweils erbrachten Tätigkeit. Die Tätigkeiten der eingesetzten Personen müssen dabei einzeln und personenbezogen erfasst werden.

Bei entsprechendem Nachweis können pro Person und pro Kalendertag bis zu 10 Stunden abgerechnet werden.

Im Laufe des Projektes können in Abstimmung zwischen AN und AG bei Bedarf Personentage auftragswertneutral zwischen den einzelnen (beauftragten) AP verschoben werden.

Abrufe aus diesem Kontingent erfolgen durch den AG in Textform. Der AN erstellt für den jeweiligen Abruf eine Kalkulation der Personentage. Erst nach Freigabe dieser Kalkulation durch den AG gilt der Abruf als getätigt. Leistungen, die außerhalb des Abrufs geleistet werden, werden nicht vergütet. Sollte das Abrufziel ohne Erfüllung zusätzlicher Leistungen/Personentage nicht erreicht werden können, ist dies unverzüglich nach Kenntnisnahme dem AG zu kommunizieren. Nach Prüfung durch den AG erfolgt ggf. eine Aufstockung der für den betroffenen Abruf zur Verfügung stehenden Personentage. Sollte im Rahmen eines Abrufs der tatsächliche Aufwand die vereinbarte Anzahl von Personentagen unterschreiten, werden die freien Ressourcen wieder dem verbleibenden Kontingent zugerechnet.

3.1.2.2 Lizenzkosten

Für die in AP 2 anfallenden Lizenzkosten legt der AG eine maximale Obergrenze von insgesamt 25.000 € (zzgl. USt) fest. Die Beschaffung der notwendigen Lizenzen erfolgt durch den AN.

Die tatsächlich angefallenen Lizenzkosten sind bei Rechnungsstellung durch Vorlage von Scans/digitalen Kopien der Originalrechnungen zu belegen. Es können nur die in den Originalrechnungen aufgeführten Nettobeträge zzgl. der für die Hauptleistung dieses Auftrages geltenden Umsatzsteuer geltend gemacht werden.

Es ist durch den AN mindestens eine Internetrecherche bzw. ein formloser Preisvergleich durchzuführen. Die Beschaffung erfolgt durch den AN beim Anbieter mit dem wirtschaftlichsten Angebot. Die Einhaltung der Regelungen des Kapitels 3.1.2.2 dieser Leistungsbeschreibung kann durch den AG geprüft werden und ist auf Anforderung vom AN nachzuweisen. Der AN hat daher jeden Beschaffungsvorgang sorgfältig zu dokumentieren und eine sparsame und wirtschaftliche Mittelverwendung nachzuweisen. Handelt der AN ohne ordnungsgemäße Freigabe, sind die Kosten der Beschaffung vom AN selbst zu tragen. Der AN muss Rabatte, Skonti oder sonstige Vergünstigungen, die ihm von Dritten gewährt werden, in Anspruch nehmen und in vollem Umfang an den AG weiterreichen.

- Beschaffung im Namen und auf Rechnung des AN:

Unterliegt das zu beschaffende Testprodukt mindestens dem gleichen Umsatzsteuersatz wie die vom AN im Rahmen dieses Projektes zu erbringende Hauptleistung, so beschafft der AN das Testprodukt direkt im Namen und auf Rechnung des AN.

- Beschaffung im Namen und auf Rechnung des AG (BSI):
 - Unterliegt das zu beschaffende Testprodukt einem günstigeren Umsatzsteuersatz (z. B. 7 %) als die vom AN im Rahmen dieses Projektes zu erbringende Hauptleistung (z. B. 19 %), so beschafft der AN das Testprodukt direkt im Namen und auf Rechnung des AG (mit Lieferanschrift des AN). Auf der Rechnung des Herstellers / des Lieferanten ist der AG (BSI) zwingend als Rechnungsempfänger zu nennen. Die Zahlung der Rechnungsbeträge an die Hersteller / die Lieferanten erfolgt durch den AG. Es ist außer in mit dem AG abgestimmten Ausnahmefällen ein Zahlungsziel von 30 Tagen zu vereinbaren. Der AG hält für die Begleichung dieser Rechnungen ein ausreichendes Budget bereit.
 - Der AG ist unverzüglich über den Eingang der Ware und die Mangelfreiheit bzw. die bestehenden Mängel zu informieren.
- Für alle Beschaffungen ist eine Freigabe durch den AG erforderlich.

Die beschafften Lizenzen sind dem AG nach Abschluss der entsprechenden Tests, spätestens jedoch zum Projektende dem AG zu übergeben bzw. zu übereignen oder den Restwert an den Auftraggeber auszukehren.

Sämtliche Lizenzen sind grundsätzlich so zu wählen, dass dem AG nach Projektabschluss keine weiteren Lizenzkosten entstehen. Abweichungen hiervon sind nur nach Zustimmung des AG möglich.

3.2 Projektverlauf, Zahlungs- und Meilensteinplan

Die Projektlaufzeit beginnt mit dem Datum der Auftragserteilung (Projektstart) und endet 6 Kalenderwochen nach der durch den AN im Angebot festgelegten Dauer für die Auftragsdurchführung. Für die Fertigstellung des Projektes wird vom AG dabei ein Zeitrahmen von maximal 8 Kalendermonaten verbindlich vorgegeben, inklusive der Zeit, die ggf. für die Beauftragung der optionalen Arbeitspakete durch den AG benötigt wird. Bei einer Auftragsänderung verschiebt sich das Projektende entsprechend der Änderung. Bei erforderlichen Nachbesserungen endet die Projektlaufzeit erst mit vollständiger Abnahme der Gesamtleistung.

Kam es bei der Auftragserteilung zu zeitlichen Verschiebungen (vgl. Kapitel 6.2.1.4, Zuschlagskriterium 2.5 „Zahlungs- und Meilensteinplan“), so werden die daraus ggf. resultierenden Terminverschiebungen verbindlich zwischen AN und AG abgestimmt. Die Terminverschiebungen müssen sich innerhalb der Projektlaufzeit befinden. Der aktualisierte Meilensteinplan ist vom AN mit dem Besprechungsprotokoll, jedoch spätestens 6 Kalenderwochen nach der Auftragserteilung schriftlich oder in Textform vorzulegen. Nach Freigabe durch die BSI-Projektleitung (in Textform) wird der aktualisierte Meilensteinplan Vertragsbestandteil. Liegt innerhalb von 6 Kalenderwochen kein abgestimmter geänderter Meilensteinplan vor, so bleibt der mit dem Angebot vorgelegte Meilensteinplan gültig.

Die Auftaktbesprechung ist seitens des AN in Abstimmung mit dem AG spätestens vier Kalenderwochen nach Auftragserteilung anzusetzen.

AP 2 und 3 müssen spätestens 4 Monate nach dem offiziellen Projektstart abgeschlossen werden.

Manche Arbeitspakete bauen aufeinander auf und sind daher zwingend nacheinander zu bearbeiten. Bei den optionalen Arbeitspaketen 5, 6 und 7 ist eine (teilweise) parallele Bearbeitung möglich. Sie sind jedoch nach den Arbeitspaketen 1, 2, 3 und 4 zu beginnen und hängen von den dort durchgeführten Arbeiten ab (siehe auch Kapitel 1.4). Ein früherer Start ist in Absprache mit dem AG möglich, wenn entsprechende Ergebnisse aus den AP 2 und 3 vorliegen. Um einen planmäßigen Start der optionalen Arbeitspakete zu ermöglichen, ist vorgesehen, dass die weitere Beauftragung mindestens zwei Wochen vor dem geplanten Start des jeweiligen Arbeitspakets durch die Projektleitung im BSI in die Wege geleitet wird.

Jedes der Arbeitspakete wird einem Meilenstein zugeordnet. Ein Meilenstein gilt als erreicht, sobald die ihm zugeordneten Arbeitspakete erbracht und vom AG abgenommen wurden. Grundsätzlich können nur vollständig erbrachte Arbeitspakete abgenommen werden. Eine Rechnungslegung ist erst nach Erreichen eines Meilensteins zulässig (siehe auch Kapitel 4.11). Der Rechnung sind die Abnahmeprotokolle für die Arbeitspakete bzw. das Abnahmeprotokoll für den Meilenstein sowie die erforderlichen Belege (siehe Kapitel 3.1.2.1 und Kapitel 3.1.2.2) beizufügen.

Arbeitspaket (AP) / Meilenstein (MS)	(Kurz-) Bezeichnung	Termin nach Projektstart [Kalendermonate]		Beginn	Ende	Art der Vergütung
		Beginn	Ende			
AP 1	Auftaktbesprechung	0	1	---	<i>Datum</i>	Festpreis
MS 1	Meilenstein 1	---	1	---	<i>Datum</i>	---
AP 2	Studie zu KI im SSDLC	0	3	<i>Datum</i>	<i>Datum</i>	Aufwand
	Lizenzkosten	---	---	---	---	Aufwand
MS 2	Meilenstein 2	---	3	---	<i>Datum</i>	---
AP 3	Best Practices und PoC	2	4	<i>Datum</i>	<i>Datum</i>	Aufwand
MS 3	Meilenstein 3	---	4	---	<i>Datum</i>	---

Arbeitspaket (AP) / Meilenstein (MS)	(Kurz-) Bezeichnung	Termin nach Projektstart [Kalendermonate]		Beginn	Ende	Art der Vergütung
		Beginn	Ende			
AP 4	Zwischenworkshop	4	4	<i>Datum</i>	<i>Datum</i>	Festpreis
MS 4	Meilenstein 4	---	4	---	<i>Datum</i>	---
AP 5 (optional)	Aktualisierung Einordnung CC- Bewertungsmetrik	5	8	<i>Datum</i>	<i>Datum</i>	Aufwand
MS 5	Meilenstein 5	---	8	---	<i>Datum</i>	---
AP 6 (optional)	Guideline: KI-Tools zur Evaluierung in Prüfstellen	5	8	<i>Datum</i>	<i>Datum</i>	Aufwand
MS 6	Meilenstein 6	---	8	---	<i>Datum</i>	---
AP 7 (optional)	Referenzarchitektur KI-Tools im SSDLC in Open CoDE	5	8	<i>Datum</i>	<i>Datum</i>	Aufwand
MS 7	Meilenstein 7	---	8	---	<i>Datum</i>	---
AP 8 (optional)	Abschlussworkshop	8	8	<i>Datum</i>	<i>Datum</i>	Festpreis
MS 8	Meilenstein 8	---	8	---	<i>Datum</i>	---
Gesamtprojekt		0	8	<i>Datum</i>	<i>Datum</i>	---

Tabelle 1 - Zahlungs- und Meilensteinplan

Der hier dargestellte und nicht vollständig befüllte Zahlungs- und Meilensteinplan dient als Übersicht über den derzeit vom AG als sinnvoll erachteten Projektverlauf. Bei den Angaben in der Spalte „Termin nach Projektstart (Beginn, Ende)“ handelt es sich um unverbindliche Schätzwerte des AG. Im Rahmen des Angebotes ist ein konkreter und verbindlicher Zahlungs- und Meilensteinplan in der obenstehenden Darstellungsform vorzulegen (siehe Kapitel 6.2.1.4, Zuschlagskriterium 2.5 „Zahlungs- und Meilensteinplan“). Dabei sind die Spalten „Beginn“ und „Ende“ zu befüllen. Die verbindlichen Vorgaben aus Kapitel 3.1 sind zwingend zu beachten.

4 Rahmen- und Ausführungsbedingungen

In diesem Kapitel sind die Rahmen- und Ausführungsbedingungen für die Projektdurchführung festgelegt. Deren Einhaltung wird durch Abgabe eines Angebotes automatisch von den Bietern bestätigt (siehe Angebotsformular, Ziffer 3 „Erklärungen des Bieters“).

4.1 Personal des Auftragnehmers

Für die Erbringung der Leistung sollten vom AN mindestens 4 (AP, 2, 3) bzw. 2 (restliche APs) Personen eingesetzt werden (inkl. Projektleitung).

4.1.1 Direktionsrecht und Disziplinargewalt

AG und AN werden durch organisatorische Maßnahmen gewährleisten, dass die jeweils von Ihnen abgestellten Personen für die Leistungserbringung ausschließlich dem Direktionsrecht und der Disziplinargewalt des jeweiligen Arbeitgebers unterstehen. Weisungen erfolgen ausschließlich im Rahmen der vereinbarten Aufgabenverteilung.

4.1.2 Qualifikationen, Erfahrungen und sonstige Anforderungen

Die zur Erbringung der Leistungen eingesetzten Personen müssen vereinbarungsgemäß, unabhängig davon jedoch mindestens dem Vertragszweck und der Aufgabenstellung entsprechend, qualifiziert sein. Unabhängig davon wird der AN gewährleisten, dass die für die Leistungserbringung vorgesehenen Personen über die Qualifikation verfügen, die mindestens seinen diesbezüglichen Angaben sowie den Anforderungen des AG im Vergabeverfahren entspricht.

Für die einzelnen vorgesehenen Rollen gelten die nachfolgend aufgelisteten Mindestanforderungen. Deren Erfüllung ist im Angebot mit geeigneten Referenzen zu belegen (siehe Kapitel 6.2.1.4).

a) Projektleitung (PL):

- Erfolgreiche Leitung von mindestens einem Forschungsprojekt im KI-Bereich, welches mit der hier zu vergebenden Leistung vergleichbar ist (hinsichtlich Dauer, Umfang und Inhalt) oder darüber hinaus geht, nachzuweisen durch mindestens eine Referenz
- Mindestens Diplom-/ Masterabschluss im mathematisch-/ informatisch- / natur-/ oder ingenieurwissenschaftlichen Bereich

b) Stellvertretende Projektleitung (PL):

- Erfolgreiche Leitung oder stellvertretende Leitung von mindestens einem Forschungsprojekt, welches mit der hier zu vergebenden Leistung vergleichbar ist (hinsichtlich Dauer, Umfang und Inhalt) oder darüber hinaus geht, nachzuweisen durch mindestens eine Referenz
- Mindestens Diplom-/ Masterabschluss im mathematisch-/ informatisch- / natur-/ oder ingenieurwissenschaftlichen Bereich

c) Teamqualifikation

Die folgenden Mindestanforderungen müssen jeweils von mindestens einer und können von verschiedenen Personen des Projektteams abgedeckt werden:

- Erfahrung in mind. zwei Forschungsprojekten mit Schwerpunkt KI
- Fachexpertise im Bereich des SSDLC
- Erfahrung in der Entwicklung, Implementierung und Nutzung von KI-Tools

-
- Relevante Programmierkenntnisse und Erfahrung mit relevanten Frameworks
 - Die Fähigkeit, technische und wissenschaftliche Sachverhalte verständlich, nachvollziehbar sowie sprachlich einwandfrei aufzubereiten und zusammenhängend darzustellen; mindestens ein Mitarbeiter muss Erfahrung in der Verfassung wissenschaftlicher Dokumente besitzen, nachzuweisen durch mind. drei Publikationen im KI-Bereich oder im Bereich der Cybersicherheit bei einschlägigen Konferenzen und/oder Fachzeitschriften, idealerweise davon mind. eine bei einer Tier-1-Konferenz
 - Generelles Wissen im Bereich der Produktevaluierung

d) alle Personen des Projektteams

- Mindestens Bachelorabschluss (oder ein vergleichbarer Abschluss) im mathematisch- / informatisch- / natur- / oder ingenieurwissenschaftlichen Bereich. Alternativ ist eine einschlägige Berufserfahrung von mindestens 5 Jahren in einem gleichwertigen Arbeitsgebiet nachzuweisen

4.1.3 Personaleinsatz und -austausch

Der AN hat zwingend mindestens das Personal einzusetzen, das er im Rahmen seines Angebots (Anlage: „Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen“) als konkret einzusetzendes Personal mit Qualifikationsprofilen angeboten hat. Unabhängig davon hat er nur solches Personal einzusetzen, das für die jeweils zu erbringende Leistung hinreichend qualifiziert ist. Für jede Person, die eingesetzt wird, hat der AN spätestens eine Woche vor dem geplanten Einsatz ein Qualifikationsprofil einzureichen, es sei denn, es liegt die jeweilige Person betreffend ein solches Qualifikationsprofil beim AG bereits vor. Ein Austausch von Personal ist nur nach vorheriger Zustimmung durch den AG zulässig.

Der AG wird seine Zustimmung im Fall eines berechtigten Grundes und wenn ein gleich- oder höherwertiger Ersatz angeboten wird erteilen. Ein berechtigter Grund liegt beispielsweise vor, wenn der Austausch aufgrund Krankheit oder Ausscheiden der betreffenden Person aus dem Unternehmen oder vergleichbarer Umstände, bedingt ist. Die Umstände sind vom AN darzulegen und plausibel zu machen. Kein berechtigter Grund ist der Einsatz der betreffenden Person in einem anderen Projekt oder ein Umzug des Standorts des Unternehmens. Die Gleichwertigkeit des Ersatzes orientiert sich anhand des für die auszutauschende Person vormals eingereichten Qualifikationsprofils, soweit ein solches vorliegt, andernfalls nach billigem Ermessen.

Eine höhere Qualifikation der Ersatzperson begründet keinen Anspruch auf Erhöhung der Vergütung.

Die durch den Austausch und die Einarbeitung der Ersatzperson entstehenden Kosten gehen zu Lasten des AN.

Das eingetauschte Personal ist unverzüglich auf Kosten des AN vollumfänglich einzuarbeiten. Soweit möglich arbeitet die ausscheidende Person die Ersatzperson ein.

4.2 Projektorganisation und Erreichbarkeit

Durch den AN ist eine qualifizierte Person als Projektleitung zur Verfügung zu stellen, die sich mit der Projektleitung des AG abstimmt und die durchzuführenden Arbeiten auf Seiten des AN koordiniert.

Die Projektleitung muss während der üblichen Arbeitszeiten (Montag bis Freitag, jeweils mindestens von 9:30 bis 15:30 Uhr) regelmäßig telefonisch oder per E-Mail erreichbar sein. Sollte die Projektleitung verhindert sein, muss jeweils eine Vertreterin oder ein Vertreter benannt werden.

Seitens des AG wird das Projekt von Referat T25 geleitet. Ansprechpartner/-innen werden bei Erteilung des Zuschlags mitgeteilt.

4.3 Projektsprache

Die Projektsprache ist grundsätzlich Deutsch. Abweichungen sind in der folgenden Tabelle aufgeführt und können in Abstimmung zwischen AG und AN erweitert oder gestrichen werden:

Ergebnisdokumente AP 2, 3, 5	Zusätzlich Englisch
Programm-Codes (z.B. bei PoC)	Kommentare Englisch

4.4 Besprechungen

Die Auftaktbesprechung (AP 1), die Präsentation der Zwischenergebnisse (AP 4) sowie die Abschlussbesprechung (AP 8) finden virtuell statt.

Zudem sind im Rahmen der Arbeitspakete AP 2, AP 3, AP 5, AP 6 und AP 7 regelmäßige, virtuelle (Video- oder Telefonkonferenz) Arbeitstreffen, etwa alle zwei Wochen, einzuplanen, um das weitere Vorgehen abzustimmen und dem AG die Möglichkeit zu geben, inhaltliche Schwerpunkte zu setzen und Feedback zu geben. Der AN berichtet in diesen regelmäßigen Besprechungen über den aktuellen Stand der Arbeiten und die geplanten inhaltlichen Aktivitäten der nächsten zwei Wochen. Darüber hinaus stattfindende Meetings zur Diskussion von Zwischenergebnissen finden nach Absprache ebenfalls virtuell statt. Der AN stellt, sofern nicht anders zwischen AG und AN vereinbart, die Plattform für die anfallenden virtuellen Treffen (Videokonferenzen).

Zu jedem Arbeitstreffen ist ein schriftliches Protokoll durch den AN anzufertigen, in dem die Beschlüsse und Ergebnisse festgehalten werden. Das Protokoll ist dem AG, sofern nicht anders vereinbart, spätestens drei Arbeitstage nach Stattfinden des jeweiligen Arbeitstreffens zur Freigabe vorzulegen.

Struktur und Format der Besprechungsprotokolle werden im Rahmen der Auftaktbesprechung festgelegt. Abweichungen von den vereinbarten Regelungen zu den Besprechungen und der entsprechenden Protokollierung bedürfen der Zustimmung des AG.

4.5 Berichtswesen

Im Rahmen des Berichtswesens erhält der AG vom AN alle 14 Tage einen tabellarischen, fortlaufend zu erweiternden und aussagekräftigen Kurzbericht per E-Mail über den Verlauf. Mögliche Probleme im Projektverlauf sind sofort anzuzeigen und dem AG gegenüber besonders hervorzuheben. Die vertraglichen Regelungen in Ziffer 9 des Projektvertrages bleiben unberührt.

Struktur und Format der regelmäßigen Berichte werden im Rahmen der Auftaktbesprechung festgelegt.

Abweichungen vom vereinbarten Berichtswesen sind möglich, bedürfen jedoch der Zustimmung des BSI.

4.6 Formale Anforderungen an Projektdokumente

Der AN übermittelt die Projektdokumente (Projektergebnisse, Besprechungsprotokolle, Berichte) in elektronischer Form entweder im Open XML-Dateiformat (DOCX) oder im Portable Document-Format (PDF) an den AG. Wurde sich auf die Erstellung von Microsoft Word-Dokumenten geeinigt, so ist in diesen grundsätzlich auf die Referenzierung von OLE-Objekten (Object Linking and Embedding) zu verzichten. Ausnahmen von diesen Dateiformaten und Regelungen sind erst nach Absprache mit dem AG möglich. Die Ergebnisdokumente aus AP 2, AP 3, AP 5 und AP 6 sind dem AG sowohl in editierbarer Form als auch als PDF-Datei vorzulegen.

Alle Projektdokumente sind übersichtlich strukturiert und enthalten (wenn sinnvoll) ein Inhaltsverzeichnis, eine Zusammenfassung, eine Dokumenten-Version, eine Änderungshistorie mit Erstellungs- und

Bearbeitungs-Datum sowie der Liste der Autoren, so dass Erstellung und Änderung des jeweiligen Dokuments nachvollziehbar sind. Sämtliche Dateien – unabhängig vom Dateityp, d.h. sowohl Open XML, Portable Document, als auch Bilddatei etc.– müssen vom AN von Metadaten bereinigt werden. Es dürfen in den Metadaten weder personenbezogene Daten enthalten sein, noch Informationen zur eingesetzten Software.

Die sprachliche Qualität ist von großer Bedeutung. Im Durchschnitt sind pro Textseite maximal vier sprachliche Fehler, das heißt grammatikalische Fehler oder Rechtschreibfehler, zulässig.

Zudem ist darauf zu achten, dass mindestens Ergebnisdokumente, welche (möglicherweise) zur Veröffentlichung vorgesehen sind, in geschlechtergerechter Sprache zu erstellen sind. Dabei sind mindestens die Anforderungen für Gesetzestexte (siehe Handbuch der Rechtsförmlichkeit des BMJ: http://hdr.bmj.de/page_b.1.html#an_110) zu erfüllen, es dürfen jedoch nur die offiziell zugelassen Möglichkeiten der deutschen Sprache (also kein Genderstern, Doppelpunkt oder Unterstrich) verwendet werden.

4.7 Barrierefreie Gestaltung

Die folgenden Projektdokumente / Lieferleistungen sind barrierefrei zu erstellen:

- Publikation der Ergebnisse von AP 2, AP 3 und AP 5
- Guideline aus AP 6
- Umsetzungsplan aus AP 7

Dabei sind die Vorgaben der aktuellen Barrierefreie-Informationstechnik-Verordnung (BITV 2.0, https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html) zwingend einzuhalten.

Da sich nur ein von Anfang an gut strukturiertes Dokument ohne größere Probleme in ein barrierefreies PDF umwandeln lässt, ist bereits das Dokument in seinem editierbaren Ursprungsformat barrierefrei zu erstellen. Im Autorendokument (Word) dürfen hierzu durch die softwareeigene Prüfung keine Fehler angezeigt werden. Folgende Anforderungen an das PDF-Endprodukt sind zu erfüllen:

1. Das PDF-Dokument muss für handelsübliche Screenreader geeignet sein und sinnvoll vorgelesen werden können.
2. **Das PDF-Dokument muss die Prüfung nach PDF/UA durch den PDF Accessibility Checker (PAC) fehlerfrei bestehen** (kostenfreies Tool zur Verwendung auf Windows-PCs).
3. PDFs müssen durch Lesezeichen strukturiert sein.
4. Das Dokument muss über ein getaggttes Inhaltsverzeichnis sowie eine korrekte Überschriftenstruktur verfügen.
5. Die Dokumenteigenschaften müssen fehlerfrei eingetragen und konfiguriert sein (Hauptsprache, Titel, Autor, Tags, Kommentare).
6. Die Lesereihenfolge und die Tag-Struktur müssen sinnvoll angeordnet sein.
7. Alle Bilder (Ausnahme: Hintergrundgrafiken/Artefakte) müssen sinnvolle Titel und Alternativtexte (Bildbeschreibung – keine Bildunterschrift) haben.
8. Bilder und Texte müssen im Wesentlichen kontrastreich verarbeitet werden (z. B. keine dunkle Schrift auf dunklem Hintergrund, gut differenzierbare Verwendung von Farben in Diagrammen, etc.).
9. Listenelemente müssen (auch seitenübergreifend) sinnvoll gegliedert sein
10. Tabellen müssen korrekt ausgezeichnet (Kopfzeilen, Lesereihenfolge) und strukturiert (TH, TD, Colspan, Rowspan) sein.
11. Seitenübergreifende Tabellen müssen als eine Tabelle erkannt werden.
12. Linkverweise zu Webseiten (insbesondere Mehrzeilige) müssen auf korrekte Funktionsweise getestet werden.
13. Die Schriften müssen korrekt im PDF eingebettet sein als „eingebettete Untergruppe“.

Eine Erläuterung der gesetzlichen Prüfroutine mit allen Details und Hinweisen für Web und PDF-Dateien findet sich unter <https://bitvtest.de/test-methodik/web/beschreibung-des-pruefverfahrens>.

4.8 Verschlüsselung der Kommunikation

Im Rahmen dieses Projektes erfolgt die E-Mail-Kommunikation (Versand und Empfang) verschlüsselt und signiert nach dem OpenPGP- oder S/MIME-Standard.

Ein Schlüsselaustausch erfolgt im Rahmen der Auftaktbesprechung. Der AN hat dafür Sorge zu tragen, dass der Schlüssel nur auf den zugelassenen Wegen an die Personen des Projektteams verteilt wird.

4.9 Berechtigte Interessen des Herstellers

Zur Untersuchung von informationstechnischen Produkten und Systemen darf sich das BSI gemäß § 7a Abs. 2 BSIG externer Auftragnehmer nur bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen. Die Beauftragung eines direkten Konkurrenten (sonstige Hersteller von KI-Tools, die unmittelbar für den Einsatz im Kontext des SSDLC entwickelt wurden) mit der hier beschriebenen Leistung ist somit ausgeschlossen.

Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen seitens des BSI weitergegeben bzw. veröffentlicht werden, soweit dies zur Erfüllung der in § 7a Abs. 2 BSIG genannten Aufgaben erforderlich ist. Vor der Weitergabe bzw. Veröffentlichung der Informationen gibt das BSI dem betroffenen Hersteller unter Berücksichtigung einer angemessenen Frist vorab Gelegenheit zur Stellungnahme.

Nach Abschluss des Projektes sind alle bei der Durchführung des Projektes angefallenen Dokumente und Ergebnisse an das BSI herauszugeben und anschließend beim AN zu löschen. Die Löschung ist dem BSI gegenüber glaubhaft zu machen.

4.10 Einsatz von Unterauftragnehmern

Der AN kann zur Leistungserbringung Unterauftragnehmer nur einsetzen oder eingesetzte Unterauftragnehmer nur auswechseln, wenn der AG dem ausdrücklich vorher zustimmt. Die Zustimmung kann nicht aus sachwidrigen Gründen verweigert werden.

Die Einarbeitung des neuen Unterauftragnehmers erfolgt auf Kosten des AN. Für die im Angebot des AN benannten Unterauftragnehmer gilt die Zustimmung des AG als erteilt.

Die Weitergabe von Projektteilen an nicht zugelassene Unterauftragnehmer ist verboten.

4.11 Anforderungen an die Rechnungsstellung

4.11.1 Zeitpunkt

Um dem AG eine ordnungsgemäße Bewirtschaftung der ihm vom Gesetzgeber zugewiesenen Haushaltsmittel zu ermöglichen, sind die vom AN erbrachten Leistungen frühestmöglich nach Eintreten des entsprechenden vertraglich vereinbarten Meilensteins, spätestens jedoch 30 Kalendertage nach dessen Eintreten, in Rechnung zu stellen.

Bei abnahmefähigen Leistungen setzt das Eintreten eines Meilensteines eine erfolgreiche Abnahme voraus.

4.11.2 Elektronische Form

Gemäß § 3 i.V.m. § 11 der E-Rechnungsverordnung (E-RechV) sind Rechnungen zwingend in elektronischer Form auszustellen und zu übermitteln. Hierbei ist grundsätzlich der Datenaustauschstandard XRechnung in der jeweils aktuellen Fassung zu verwenden (§ 4 E-RechV).

Erforderliche Anlagen sind immer die Abnahmeprotokolle für die abzurechnenden Leistungen sowie bei Leistungen nach Aufwand zusätzlich die entsprechenden Leistungsnachweise.

Rechnungsformate, welche nicht den Anforderungen der europäischen Norm für die Rechnungsstellung (EN-16931) entsprechen sowie Rechnungen, die nicht über die Rechnungseingangsplattform des Bundes (<https://xrechnung-bdr.de>) zugestellt wurden, werden nicht berücksichtigt.

Nähere Informationen zu den formalen Anforderungen sind dem in den Vergabeunterlagen enthaltenen Dokument „Die Rechnungseingangsplattformen des Bundes“ (Version September 2025) zu entnehmen.

4.12 Nachhaltige Umsetzung der Leistung

Der AG berücksichtigt bei der Leistungserbringung Nachhaltigkeitsanforderungen, indem er bspw. Dienstreisen reduziert, nachhaltige Energienutzung anwendet, Besprechungen über elektronische Videokonferenzsysteme abhält, Papiereinsparungsmaßnahmen vornimmt und sofern möglich Müll bzw. Elektroschrott bestmöglich vermeidet.

4.13 Bundestariftreuegesetz

Gemäß § 3 des Gesetzes zur Sicherung der Tariftreue bei der Vergabe und Ausführung öffentlicher Aufträge und Konzessionen des Bundes (Bundestariftreuegesetz – BTTG) müssen Bundesauftraggeber ihren Auftragnehmer verbindlich vorgeben, dass der Auftragnehmer die zur Leistungserbringung eingesetzten Arbeitnehmerinnen und Arbeitnehmer für die Dauer, in der sie in Ausführung des öffentlichen Auftrags tätig sind, mindestens die Arbeitsbedingungen gewähren muss, die die jeweils einschlägige Rechtsverordnung nach § 5 BTTG festsetzt.

Bislang ist keine solche Rechtsverordnung erlassen worden. Mit der Angebotsabgabe bestätigen Sie, dass falls eine einschlägige Rechtsverordnung erlassen wird, alle beteiligten Unternehmen ihre im Rahmen dieses Auftrags eingesetzten Arbeitnehmerinnen und Arbeitnehmer darüber informieren, dass für die Dauer des Einsatzes ihr Arbeitsverhältnis mindestens die tariflichen Arbeitsbedingungen nach der einschlägigen Rechtsverordnung, sowie nach dem Bundestariftreuegesetz einzuhalten sind.

Sie sind dann verpflichtet, mittels geeigneter Unterlagen zu dokumentieren, dass Sie ihre Tariftreueversprechen nach § 3 BTTG einhalten. Sie sind außerdem verpflichtet, diese Unterlagen auf Anforderung der Prüfstelle Bundestariftreue vorzulegen. Die Pflicht gilt nicht, sofern die Bedingungen des § 10 BTTG zutreffen. Sie müssen von Unterauftragnehmern und von ihnen oder den Unterauftragnehmern beauftragten Verleihern verlangen und durch geeignete Maßnahmen sicherstellen, dass diese ihre Pflichten nach § 4 Absatz 1 und 3 BTTG erfüllen. Keine Unterauftragnehmer sind unmittelbare oder mittelbare Zulieferer im Sinne von § 2 Abs. 5 Satz 2 Nr. 2 und § i.V.m. Abs. 7 und 8 des Lieferkettensorgfaltspflichtengesetzes, soweit diese Zulieferer keine eigene Verpflichtung des Auftragnehmers erfüllen. Verleiher sind solche nach § 1 Abs. 1 des Arbeitnehmerüberlassungsgesetzes

Stellt die Prüfstelle Bundestariftreue einen Verstoß nach § 13 Bundestariftreuegesetz fest, ist eine Vertragsstrafe in Höhe von 0,5 Prozent, bei mehreren Verstößen maximal 5 % der anteiligen Vergütung verwirkt, die für die bis zur Feststellung des Verstoßes erbrachten Leistungen geschuldet ist oder geschuldet sein wird. Das BSI hat in diesem Fall ein Recht zur außerordentlichen Kündigung.

B Besondere Bewerbungsbedingungen

5 Bedingungen für die Zuschlagserteilung

In diesem Kapitel sind die Bedingungen für die Zuschlagserteilung festgelegt, die bei der Erstellung eines Angebots gemäß Kapitel 6 zu berücksichtigen sind.

5.1 Gesetzliche Ausschlussgründe, Eignung und Ausführungsbedingungen

Öffentliche Aufträge werden nur an fachkundige und leistungsfähige (geeignete) Unternehmen vergeben, die nicht nach den §§ 123 oder 124 GWB ausgeschlossen worden sind (§ 122 Abs. 1 GWB, § 31 Abs. 1 UVgO).

Die zwingenden Ausschlussgründe (§ 123 GWB) und die fakultativen Ausschlussgründe (§ 124 GWB) können unter den folgenden Quellen nachgelesen werden:

- https://www.gesetze-im-internet.de/gwb/_123.html
- https://www.gesetze-im-internet.de/gwb/_124.html

Mit der Abgabe des Angebots erklären die Bieter, dass keine der in §§ 123, 124 GWB genannten Gründe im Hinblick auf ihre Person oder Unternehmen vorliegen, soweit nicht eine Erklärung zu den §§ 123, 124 GWB eingereicht wurde (siehe Kapitel 6.2.4). Das BSI schließt ein Unternehmen jedoch zu jedem Zeitpunkt des Vergabeverfahrens von der Teilnahme aus, wenn es Kenntnis davon erhält, dass ein Ausschlussgrund nach § 123 GWB vorliegt. Ein Ausschluss kommt gleichermaßen bei Kenntnis über einen Ausschlussgrund nach § 124 GWB in Betracht. Die Möglichkeit der Selbstreinigung nach § 125 GWB bleibt unberührt.

Das BSI prüft, ob die Bieter die festgelegten Eignungskriterien (siehe Kapitel 6.2.1.3) und etwaig festgelegte Mindestanforderungen erfüllen (§ 122 Abs. 2 GWB⁴, § 31 Abs. 2 UVgO). Wird eine Mindestanforderung an die Eignung nicht erfüllt, ist das Angebot auszuschließen. Im Übrigen prüft das BSI auf Grundlage der Eignungskriterien, ob die vorgelegten Belege den Schluss zulassen, dass der Bieter den Auftrag ordnungsgemäß erfüllen kann.

Ausführungsbedingungen betreffen die Vertragsausführung und stellen vom BSI festgelegte Bedingungen dar, die vom AN einzuhalten sind. Der Transparenz halber ist von den Bietern bereits im Vergabeverfahren zu versichern, dass sie im Rahmen der Auftragsausführung die vom BSI vorgesehenen Bedingungen einhalten werden (siehe Angebotsformular, Ziffer 3 „Erklärungen des Bieters“).

5.2 Wirtschaftlichstes Angebot

Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt. Grundlage dafür ist eine Bewertung des BSI, ob und inwieweit das Angebot die vorgegebenen Zuschlagskriterien erfüllt. Das wirtschaftlichste Angebot bestimmt sich nach dem besten Preis-Leistungs-Verhältnis. Zu dessen Ermittlung können neben dem Preis oder den Kosten auch qualitative, umweltbezogene oder soziale Aspekte berücksichtigt werden (§ 127 Abs. 1 GWB, § 43 Abs. 1 und 2 UVgO).

Für die Ermittlung der Wirtschaftlichkeit eines Angebotes wendet das BSI die „erweiterten Richtwertmethode“ über die Faktoren „Bewertungspreis“ (siehe Kapitel 5.2.1) und „Leistung“ (siehe Kapitel 5.2.2) an.

⁴ Jeweils in Verbindung mit den Regelungen der §§ 42 ff. VgV oder §§ 7, 21 ff VSVgV.

5.2.1 Bewertungspreis

Der Bewertungspreis umfasst die folgenden Komponenten (siehe auch Kapitel 6.1):

Bewertungspreis =	Angebotsnettopreis + anfallende (Einfuhr-/)Umsatzsteuer ohne Rücksicht auf die Steuerschuldnerschaft
-------------------	--

Der Angebotsnettopreis umfasst dabei sämtliche Einzelpositionen (siehe Kapitel 3.2, Tabelle 1).

5.2.2 Leistung

Die „Leistung“ der einzelnen Angebote wird vom BSI anhand der festgelegten qualitativen Zuschlagskriterien (siehe Kapitel 6.2.1.4) bewertet.

Bei den qualitativen Zuschlagskriterien wird zwischen Ausschlusskriterien (**A**-Kriterien) und Bewertungskriterien (**B**-Kriterien) differenziert.

Während bei einem A-Kriterium lediglich geprüft wird, ob die Ausführungen des Bieters die definierten Mindestanforderungen erfüllen (Prüfergebnis: Ja oder Nein), werden die Ausführungen des Bieters bei einem B-Kriterium anhand einer durchgängigen Wertungsskala von 0 bis 4 Bewertungspunkten (**BP**) bewertet:

BP	Zielerreichungsgrad
0	Es sind keine Angaben vorhanden oder in Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI nur in unzureichendem Maße entsprechen wird.
1	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI in ausreichendem Maße entsprechen wird.
2	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI weitgehend entsprechen wird.
3	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI voll entsprechen wird.
4	In Bezug auf das abgefragte Kriterium lassen die Ausführungen erwarten, dass die Auftragsausführung den Anforderungen des BSI in besonderem Maße entsprechen wird.

Zur Orientierung werden bei jedem B-Kriterium die Voraussetzungen angegeben, die erfüllt sein müssen, damit das Angebot bzgl. dieses Kriteriums vom BSI mit 0 BP, 1 BP oder 4 BP bewertet wird. Die Bewertung bei Kriterium 2.1 richtet sich allein nach dem in Kapitel 6.2.1.4 Kriterium 2.1 angegebenen Wertungsmaßstab.

Bei den B-Kriterien muss das Angebot jeweils mindestens 1 BP (**BP_{min}** = 1) erzielen (Mindestanforderung).

Erfüllt ein Angebot bei mindestens einem A-Kriterium oder bei mindestens einem B-Kriterium nicht die definierte Mindestanforderung, so wird dieses Angebot von der Wertung ausgeschlossen.

Bei den verbleibenden Angeboten ergeben sich die für die erweiterte Richtwertmethode maßgeblichen Leistungspunkte (**LP**) aus dem Produkt der bei den einzelnen B-Kriterien erzielten BP und der vom BSI für die jeweiligen B-Kriterien vorgegebenen Gewichtungsfaktoren (**GF**, siehe Kapitel 6.2.1.4).

5.2.3 Erweiterte Richtwertmethode mit dem Entscheidungskriterium „Leistungspunkte“

Bei der erweiterten Richtwertmethode wird in einem ersten Schritt für jedes der Angebote eine individuelle Kennzahl, welche aus dem Quotient zwischen den erzielten Leistungspunkten (siehe Kapitel 5.2.2) und dem Bewertungspreis (siehe Kapitel 5.2.1) besteht, ermittelt.

Ausgehend vom Angebot mit der höchsten Kennzahl wird in einem nächsten Schritt ein Schwankungsbereich von 10 % definiert. Alle Angebote, die mit Ihrer Kennzahl unterhalb dieses Schwankungsbereiches liegen, können bei der Zuschlagserteilung nicht berücksichtigt werden.

Bei den verbleibenden Angeboten erfolgt die Zuschlagserteilung auf das Angebot mit der höchsten Leistungspunktzahl. Ist die Leistungspunktzahl identisch, erfolgt der Zuschlag auf das preislich günstigere Angebot.

6 Erstellung des Angebots

Ein vollständiges Angebot besteht aus folgenden Unterlagen:

- Angebotsformular (siehe Kapitel 6.1)
- Anlagen zum Angebotsformular
- Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen (siehe Kapitel 6.2.1). Wird im Rahmen einzelner Eignungskriterien und / oder Zuschlagskriterien explizit die Einreichung weiterer Dokumente (z.B. Kopie einer offiziellen Bescheinigung oder eines amtlichen Nachweises, etc.) gefordert, so sind diese nach Möglichkeit an der entsprechenden Stelle in diese Anlage zu integrieren. Ist eine Integration nicht möglich, so bilden diese eine eigenständige Anlage.
- ggf. Bietergemeinschaftserklärung (siehe Kapitel 6.2.2)
- ggf. Unterauftragnehmerverspflichtungserklärung (siehe Kapitel 6.2.3)
- ggf. Angaben zu vorliegenden Ausschlussgründen und zur Selbstreinigung im Sinne von § 125 GWB (siehe Kapitel 6.2.4)
- ggf. weitere individuelle Anlagen des Bieters (siehe Kapitel 6.2)

Die Anzahl der geforderten Anlagen ist dabei abhängig von der Bieterkonstellation (siehe Kapitel 6.2.2), der geplanten Einbindung von Unterauftragnehmern (siehe Kapitel 6.2.3) sowie dem Vorliegen von gesetzlichen Ausschlussgründen (siehe Kapitel 6.2.4).

Das BSI ist rechtlich verpflichtet, die eingereichten Angebote mindestens drei Jahre ab dem Tag der Zuschlagserteilung aufzubewahren. Reichen Sie daher alle für die Angebotswertung relevanten Informationen in archivierbarer Form ein. Verzichten Sie z.B. in der Anlage „Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen“ auf die Angabe von URLs bzw. auf deren Verweisung.

Bitte fügen Sie nach Möglichkeit alle Anlagen zum Angebotsformular zu einer „Gesamtdatei“ (PDF) zusammen (jedoch ohne das Angebotsformular, vgl. Kapitel 6.1).

6.1 Angebotsformular

Das in den Vergabeunterlagen enthaltene Angebotsformular ist gemäß den dort aufgeführten Vorgaben auszufüllen.

Ist die Steuerschuldnerschaft aufgrund von § 13b UStG auf den AG übergegangen (reverse charge), so weisen Sie im Angebot einen Steuersatz von 0 % aus. In diesem Fall wird die von AG abzuführende Umsatzsteuer bei der Bewertung des Angebotes berücksichtigt (siehe Kapitel 5.2.1).

Verschiedene Eingabefelder des Angebotsformulars werden nach Abgabe und Öffnung des Angebotes maschinell ausgelesen. Verzichten Sie daher auf die Einreichung eines eingescannten Auftragsformulars und auf die Zusammenfassung des Angebotsformulars mit den zugehörigen Anlagen zu einer „Gesamtdatei“.

6.2 Anlagen zum Angebotsformular

Die nachfolgenden Unterkapitel geben einen Überblick über die einzelnen Anlagen sowie über deren inhaltliche Anforderungen.

Falls aus Sicht des Bieters erforderlich, so kann das Angebot um weitere Anlagen ergänzt werden.

Alle zum Angebot gehörenden Anlagen sind auf Seite 2 des Angebotsformulars aufzuführen.

6.2.1 Anlage: Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen

Die von jedem Bieter individuell zu erstellende Anlage „Angebotsangaben gemäß den Besonderen Bewerbungsbedingungen“ fungiert neben dem Angebotsformular als zentraler Bestandteil des Angebotes.

Halten Sie sich bei der Erstellung dieser Anlage an die Vorgaben in den Kapiteln 6.2.1.1 bis 6.2.1.4 sowie an die vorgegebene Reihenfolge. Achten Sie darauf, die geforderten Angaben unmittelbar bei den einzelnen Kriterien aufzuführen.

Achtung: Verzichten Sie auf nicht geforderte Angaben, insbesondere zu den vertraglichen Regelungen (siehe Ziffer 4.2 der Allgemeinen Bewerbungsbedingungen).

Die vollständige Abdeckung des in der Leistungsbeschreibung geforderten Leistungsumfangs inkl. der Einhaltung sämtlicher in Kapitel 4 der Leistungsbeschreibung definierten Rahmen- und Ausführungsbedingungen wird durch Abgabe eines Angebotes automatisch bestätigt (siehe Angebotsformular, Ziffer 3 „Erklärungen des Bieters“).

6.2.1.1 Einzelbieter / Mitglieder der Bietergemeinschaft

Erstellen Sie vom Einzelbieter bzw. vom jedem Mitglied der Bietergemeinschaft ein aussagekräftiges Firmenprofil. Die Darstellung muss in tabellarischer Form erfolgen und folgende Punkte umfassen:

- Offizielle Bezeichnung
- Rechtsform
- Firmensitz und Standorte
- Struktur und Organisation
- z.B. Abbildung des Organigramms
- Geschäftsfelder
- Auflistung der einzelnen Geschäftsfelder
- Benennung der Geschäftsfelder, die für den hier zu vergebenden Auftrag relevant sind (auftragsbezogene Geschäftsfelder)
- ggf. nähere Ausführungen / Erläuterungen zu den auftragsbezogenen Geschäftsfeldern
- Anzahl der Mitarbeiter in den auftragsbezogenen Geschäftsfeldern
- Gesamtumsatz in den letzten drei Geschäftsjahren (Angabe pro Jahr), sofern entsprechende Angaben verfügbar sind.
- Umsatz in den auftragsbezogenen Geschäftsfeldern in den letzten drei Geschäftsjahren (Angabe pro Jahr), sofern entsprechende Angaben verfügbar sind.

Gehen Sie im Falle einer Bietergemeinschaft zudem auf die Aufteilung der zu erbringenden Leistung auf die einzelnen Mitglieder der Bietergemeinschaft ein.

6.2.1.2 Unterauftragnehmer

- Werden wesentliche Teile der angebotenen Leistung von einem oder mehreren Unterauftragnehmern erbracht (siehe Ziffer 2.1 des Angebotsformulars), so sind diese Unternehmen inkl. der von ihnen durchzuführenden Leistungen genau zu benennen. Erstellen Sie von jedem Unterauftragnehmer zudem ein aussagekräftiges Firmenprofil inkl. der folgenden Angaben:

- Offizielle Bezeichnung
- Rechtsform
- Firmensitz und Standorte
- auftragsbezogene Geschäftsfelder
- Anzahl der Mitarbeiter in den auftragsbezogenen Geschäftsfeldern
- durchzuführende Leistungen

Wird die Leistung ohne Mitwirkung von einem oder mehreren Unterauftragnehmern erbracht, so geben Sie an dieser Stelle Ihres Angebotes bitte lediglich „Kein Unterauftragnehmer“ an.

Die Weitergabe von wesentlichen Projektteilen an nicht genannte Unterauftragnehmer ist verboten.

6.2.1.3 Eignungskriterien

Nr.	Kriterien
1	<u>Eigenerklärung zu Artikel 5k der Verordnung (EU) 833/2014</u> Im Rahmen des EU-Sanktionspakets im Zusammenhang mit dem Angriffskrieg Russlands auf die Ukraine wurde durch Verordnung (EU) 2022/1269 des Rates vom 27.04.2023 folgender Artikel in die Verordnung (EU) 833/2014 aufgenommen: <i>Artikel 5k</i> <i>(1) Es ist verboten, öffentliche Aufträge oder Konzessionen, die in den Anwendungsbereich der Richtlinien über die öffentliche Auftragsvergabe sowie unter Artikel 10 Absatz 1, Absatz 3, Absatz 6 Buchstaben a bis e, Absatz 8, Absatz 9 und Absatz 10 und die Artikel 11, 12, 13 und 14 der Richtlinie 2014/23/EU, unter Artikel 7 Buchstaben a bis d, Artikel 8, Artikel 10 Buchstaben b bis f und h bis j der Richtlinie 2014/24/EU, unter Artikel 18, Artikel 21 Buchstaben b bis e und g bis i, Artikel 29 und Artikel 30 der Richtlinie 2014/25/EU sowie unter Artikel 13 Buchstaben a bis d, f bis h und j der Richtlinie 2009/81/EG fallen, an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen:</i> <i>a) russische Staatsangehörige, in Russland ansässige natürliche Personen oder in Russland niedergelassene juristische Personen, Organisationen oder Einrichtungen,</i> <i>b) juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50 % unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, oder</i> <i>c) natürliche oder juristische Personen, Organisationen oder Einrichtungen, die im Namen oder auf Anweisung einer der unter Buchstabe a oder b genannten Organisationen handeln,</i> <i>einschließlich – wenn auf sie mehr als 10 % des Auftragswerts entfällt – Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Sinne der Richtlinien über die öffentliche Auftragsvergabe in Anspruch genommen werden.</i> Bestätigen Sie, dass keine der o.g. Ausschlussgründe für eine öffentliche Auftragsvergabe oder Konzessionsvergabe bzw. eine Vertragsweiterführung auf Sie zutreffen und dass Sie auch im Rahmen der Vertragsausführung keine Änderungen vornehmen (z.B. durch Einbindung eines Unterauftragnehmers oder eines Lieferanten), die gegen die o.g. Ausschlussgründe verstoßen? Bitte die Frage nur mit „JA“ (→ Bestätigung) oder „NEIN“ (→ keine Bestätigung) beantworten. <u>Mindestanforderung:</u> Die Frage wurde mit „Ja“ beantwortet. Wurde die Frage mit „Nein“ beantwortet, so führt dies zum Ausschluss aus dem Vergabeverfahren. Ihnen ist bewusst, dass eine wissentlich

Nr.	Kriterien
	falsche Angabe der Erklärung zum Ausschluss aus dem Vergabeverfahren führt und nach Vertragsschluss den AG zur außerordentlichen Kündigung berechtigt. Führen Sie im Angebot lediglich den Titel des Kriteriums sowie Ihre Antwort auf. Verzichten Sie auf die wörtliche oder sinngemäße Zitierung des Kriteriums.
2	<u>Ausschluss eines Interessenskonflikts</u> Bestätigen Sie, dass weder Sie noch Ihre Partner im Fall einer Bietergemeinschaft noch ggf. Unterauftragnehmer Interessen haben, die mit der Ausführung der Leistungen dieses Projekts im Widerspruch stehen und die sich ggf. nachteilig auf das Projektergebnis auswirken könnten? Eingeschlossen von dieser Bestätigung ist das bei dem Projekt eingesetzte Personal. Bitte mit „JA“ oder „NEIN“ beantworten. Ein Interessenskonflikt liegt beispielsweise bei einer Verpflichtung gegenüber oder Kooperation mit dem Hersteller eines untersuchten Produkts oder durch eine sonstige wirtschaftliche Abhängigkeit vom genannten vor. Beispielsweise kann ein Interessenskonflikt bestehen, wenn der AN Hersteller eines KI-basierten Tools ist, das speziell für den Einsatz im SSDLC entwickelt wurde. In diesem Fall kann es mitunter sein, dass der AN kein Interesse daran besitzt, den Forschungsstand zum Thema KI im SSDLC objektiv und neutral zu untersuchen. <u>Mindestanforderung:</u> Wurde die Frage mit „Nein“ beantwortet (= es besteht ein Interessenskonflikt), so erläutern Sie den Konflikt und stellen Sie dar, wie Sie ihn auflösen wollen. Das Angebot kann in diesem Fall nur berücksichtigt werden, wenn der beschriebene Lösungsansatz vom BSI als ausreichend beurteilt wird. Führen Sie im Angebot lediglich den Titel des Kriteriums sowie Ihre Antwort auf. Verzichten Sie auf die wörtliche oder sinngemäße Zitierung des Kriteriums.
3	<u>Referenzen</u> Legen Sie geeignete Referenzen der beteiligten Unternehmen vor. Referenzen sind geeignet, wenn die der Referenz zu Grunde liegenden Projekte hinsichtlich der fachlichen und technischen Leistungsfähigkeit im Wesentlichen ähnliche Anforderungen an die Unternehmen gestellt haben wie die ausgeschriebene Leistung. Dies ist bei der vorliegenden Ausschreibung insbesondere, aber nicht ausschließlich gegeben bei Erfahrungen in Projekten im Bereich SSDLC sowie der Integration von KI-basierten Tools, insbesondere auf Basis von LLMs. Die genannten Referenzen müssen insbesondere die Fähigkeit der beteiligten Unternehmen auf dem Gebiet der Forschung und Entwicklung sowie die Ausarbeitung und Umsetzung innovativer Lösungen belegen. Im Wege der Referenzen ist daher nachzuweisen, dass die beteiligten Unternehmen bereits Erfahrungen in den folgenden Erfahrungsbereichen gesammelt haben: • Integration von KI-basierten Tools • Erfahrungen im Bereich der IT-Sicherheit • Erfahrung im wissenschaftlichen Arbeiten und Publizieren • Umsetzung/Realisierung eines innovativen Test- oder Pilotbetriebs von Produkten im SSDLC Gehen Sie bei der Erstellung des Referenznachweises auf die folgenden Punkte ein: • Auftraggeber inkl. Fachbereich • (detaillierte) Darstellung des Auftragsgegenstands / der Tätigkeit

Nr.	Kriterien
	• Umfang / Betroffener Erfahrungsbereich • Dauer • Auftragsvolumen Die Darstellung sollte insgesamt einen Umfang von zwei DIN A4-Seiten als digitales Dokument und in üblicher Formatierung (Calibri 11 pt für Fließtext oder vergleichbar, üblicher Zeilenabstand) nicht überschreiten. Es werden keine Referenzschreiben früherer Auftraggeber benötigt. <u>Mindestanforderung:</u> Insgesamt sind mindestens zwei geeignete Referenzen vorzulegen. Alle Erfahrungsbereiche müssen durch geeignete Referenzen belegt werden, wobei eine Referenz zur Abdeckung mehrerer Bereiche herangezogen werden darf.
4	<u>Referenzen: Marktanalyse</u> Belegen Sie anhand von Referenzprojekten, dass mindestens eines der beteiligten Unternehmen umfangreiche Kenntnisse und praktische Erfahrungen in der Planung und Durchführung von Marktanalysen und -bewertungen im Bereich der IT-Sicherheit oder KI besitzt. Gehen Sie dabei auf folgende Punkte ein: • Auftraggeber inkl. Fachbereich • Gegenstand der Marktanalyse • Umfang / Dauer Die Darstellung sollte insgesamt (ohne Artikel im PDF-Format) einen Umfang von einer DIN A4-Seiten als digitales Dokument und in üblicher Formatierung (Calibri 11 pt für Fließtext oder vergleichbar, üblicher Zeilenabstand) nicht überschreiten. Es werden keine Referenzschreiben früherer Auftraggeber benötigt. <u>Mindestanforderung:</u> In den letzten drei Jahren wurde mindestens eine Marktanalyse auf dem Gebiet der IT-Sicherheit oder KI durchgeführt. Dabei wurden mindestens eine Übersicht über relevante Produkte erstellt, geeignete Bewertungskriterien definiert und basierend auf diesen ein objektiver Vergleich der Produkte durchgeführt.
5	<u>Technische Ausrüstung</u> Geben Sie einen kurzen Überblick über das technische Equipment, welches Ihnen zur Erbringung der Aufgaben zur Verfügung steht. Beschreiben Sie, welches Equipment für welche Aufgaben eingesetzt werden soll und begründen Sie dies kurz. Gehen Sie insbesondere darauf ein, welche Hardware für KI-Tools mit potenziell hohem VRAM-Bedarf genutzt werden soll und erklären Sie, weswegen Sie der Meinung sind, dass diese ausreicht. Für die digitale Abstimmung und Präsentationen zwischen AG und AN wird außerdem ein System für Telefon- und Videokonferenzen benötigt. Geben Sie auch dazu einen kurzen Überblick über das technische Equipment, welches Ihnen zur Verfügung steht und von Ihnen zur Erbringung der hier ausgeschriebenen Leistung eingesetzt wird. <u>Mindestanforderung:</u> Der Bieter ist aus Sicht des BSI in der Lage, die hier zu vergebende Leistung mit Hilfe der beschriebenen technischen Ausrüstung erfolgreich zu erbringen.

6.2.1.4 Qualitative Zuschlagskriterien

Nr.	Kriterienart	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
1	B	KG1: Inhaltliche Auseinandersetzung mit der Leistung			9	36
1.1	B	<u>Aufgabenverständnis</u> Weisen Sie Ihr Aufgabenverständnis nach, indem Sie die Ausgangssituation, die Zielsetzung des Projektes und die erwarteten Ergebnisse mit eigenen Worten erläutern. Benennen Sie die Ihrer Ansicht nach wichtigsten Punkte zu diesem Fachthema. Der Umfang der Ausarbeitung darf zwei Seiten DIN A4 als digitales Dokument und in üblicher Formatierung (Calibri 11 pt für Fließtext oder vergleichbar, üblicher Zeilenabstand) nicht überschreiten. Konzeptteile, die über die vorgegebene Seitenanzahl hinausgehen, werden nicht bewertet. <u>Bewertungsskala (durchgängig von 0 bis 4 BP):</u> • 0 BP: Die Ausführungen fehlen, das Aufgabenverständnis ist lückenhaft oder aus Sicht des BSI nicht zielführend. • 1 BP: Die Ausgangssituation, die Projektziele und das erwartete Ergebnis sind ausreichend beschrieben. Die Ausarbeitung lässt eine Auseinandersetzung bzw. ein Verständnis der Thematik erkennen. Das Ziel des Projektes wurde hinreichend verstanden • 4 BP: Die Ausgangssituation, die Projektziele und das erwartete Ergebnis sind zutreffend beschrieben. Die Ausarbeitung lässt eine umfassende Auseinandersetzung bzw. ein tieferes Verständnis der Thematik erkennen. Das Ziel des Projektes wurde vollumfänglich verstanden.	1	2	2	8
1.2	B	<u>Vorgehensweise Marktsichtung</u> Erläutern Sie Ihre Vorgehensweise bei der Marktsichtung. Benennen Sie Produktgruppen, Anwendungsbereiche und Mechanismen, die aus Ihrer Sicht zu der in Kapitel 2 geforderten Marktsichtung einbezogen werden sollen. Welche Quellen werden Sie bei der Marktsichtung heranziehen? Der Umfang der Ausarbeitung darf eine Seite DIN A4 als digitales Dokument und in üblicher Formatierung (Calibri 11 pt für Fließtext oder vergleichbar, üblicher Zeilenabstand) nicht überschreiten. Konzeptteile, die über die vorgegebene Seitenanzahl hinausgehen, werden nicht bewertet.	1	2	2	8

Nr.	Kriterien- art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		<u>Bewertungsskala (durchgängig von 0 bis 4 BP):</u> • <u>0 BP:</u> Die Ausführungen fehlen, das Konzept für die Vorgehensweise bei der Marktsichtung ist lückenhaft oder aus Sicht des BSI nicht zielführend. • <u>1 BP:</u> Das Konzept für die Vorgehensweise bei der Marktsichtung ist vollständig dargestellt und plausibel. • <u>4 BP:</u> Das Konzept für die Vorgehensweise bei der Marktsichtung ist vollständig dargestellt und plausibel. Zudem lässt das Angebot eine tiefe Durchdringung der Problematik erkennen und macht deutlich, dass der AN die Beantwortung auf Basis einer hohen fachlichen Expertise vorgenommen hat.				
1.3	B	<u>Umsetzung Arbeitspaket 3</u> Beschreiben Sie detailliert, wie Sie im Rahmen von Arbeitspaket 3 bei der Erarbeitung der Best Practices vorgehen und welche Informationen Sie voraussichtlich in den Best Practices inkludieren werden (a). Erläutern Sie ferner Ihr geplantes Vorgehen bei der Erstellung des PoC (b). Der Umfang der Ausarbeitung darf zwei Seiten DIN A4 als digitales Dokument und in üblicher Formatierung (Calibri 11 pt für Fließtext oder vergleichbar, üblicher Zeilenabstand) nicht überschreiten. Die Darstellung zu den Best Practices (a) und dem PoC (b) sollte jeweils eine Seite nicht übersteigen. Konzeptteile, die über die vorgegebene Seitenanzahl hinausgehen, werden nicht bewertet. <u>Bewertungsskala (durchgängig von 0 bis 4 BP):</u> • <u>0 BP:</u> Die Ausführungen fehlen, sind lückenhaft, aus fachlicher Sicht unstimmtig oder der angebotene Leistungsgegenstand erfüllt aus Sicht des BSI nicht die Anforderungen der Leistungsbeschreibung. • <u>1 BP:</u> Die Ausführungen sind vollständig und stimmig. Aus Sicht des BSI können die Minimalziele dieses Projektes auf dem beschriebenen Wege erfolgreich erreicht werden. • <u>4 BP:</u> Die Ausführungen sind vollständig und stimmig. Sie lassen eine tiefe Durchdringung des Themas erkennen und zeigen Möglichkeiten für eine optimierte Bearbeitung des Arbeitspaketes. Die Darstellung der Best Practices geht deutlich	1	2	2	8

Nr.	Kriterien-art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		über die in der Beschreibung des Arbeitspakets 3 genannten Punkte (korrekte Verwendung der Tools, Umgang mit ihren Ausgaben) hinaus.				
1.4	B	<u>Umsetzung Arbeitspaket 5</u> Beschreiben Sie detailliert, wie Sie die in Arbeitspaket 5 enthaltenen Anforderungen bzgl. der Aktualisierung der Bewertungsmetrik umsetzen werden. Der Umfang der Ausarbeitung darf eine Seite DIN A4 als digitales Dokument und in üblicher Formatierung (Calibri 11 pt für Fließtext oder vergleichbar, üblicher Zeilenabstand) nicht überschreiten. Konzeptteile, die über die vorgegebene Seitenanzahl hinausgehen, werden nicht bewertet. <u>Bewertungsskala (durchgängig von 0 bis 4 BP):</u> • <u>0 BP:</u> Die Ausführungen fehlen, sind lückenhaft, aus fachlicher Sicht unstimmig oder der angebotene Leistungsgegenstand erfüllt aus Sicht des BSI nicht die Anforderungen der Leistungsbeschreibung. • <u>1 BP:</u> Die Ausführungen sind vollständig und stimmig. Aus Sicht des BSI können die Minimalziele dieses Projektes auf dem beschriebenen Wege erfolgreich erreicht werden. • <u>4 BP:</u> Die Ausführungen sind vollständig und stimmig. Sie lassen eine tiefe Durchdringung des Themas erkennen und zeigen Möglichkeiten für eine optimierte Bearbeitung des Arbeitspaketes.	1	1	1	4
1.5	B	<u>Umsetzung Arbeitspaket 7</u> Beschreiben Sie detailliert, wie Sie die in Arbeitspaket 7 enthaltenen Anforderungen bzgl. der Erstellung einer Referenzarchitektur umsetzen werden. Der Umfang der Ausarbeitung darf zwei Seiten DIN A4 als digitales Dokument und in üblicher Formatierung (Calibri 11 pt für Fließtext oder vergleichbar, üblicher Zeilenabstand) nicht überschreiten. Konzeptteile, die über die vorgegebene Seitenanzahl hinausgehen, werden nicht bewertet. <u>Bewertungsskala (durchgängig von 0 bis 4 BP):</u> • <u>0 BP:</u> Die Ausführungen fehlen, sind lückenhaft, aus fachlicher Sicht unstimmig oder der angebotene Leistungsgegenstand erfüllt aus Sicht des BSI nicht die Anforderungen der Leistungsbeschreibung.	1	1	1	4

Nr.	Kriterien-art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		• <u>1 BP</u>: Die Ausführungen sind vollständig und stimmig. Aus Sicht des BSI können die Minimalziele dieses Projektes auf dem beschriebenen Wege erfolgreich erreicht werden. • <u>4 BP</u>: Die Ausführungen sind vollständig und stimmig. Sie lassen eine tiefe Durchdringung des Themas erkennen und zeigen Möglichkeiten für eine optimierte Bearbeitung des Arbeitspaketes.				
1.6	B	<u>Projektrisiken</u> Welche Projektrisiken sehen Sie? Wie schätzen Sie diese hinsichtlich Eintrittswahrscheinlichkeit und Schadensausmaß ein? Wie werden Sie mit diesen umgehen? Stellen Sie die Beantwortung der Fragen in einer Tabelle dar. Der Umfang der Tabelle darf zwei Seiten DIN A4 als digitales Dokument und in üblicher Formatierung (Calibri 11 pt oder vergleichbar) nicht überschreiten. Konzeptteile, die über die vorgegebene Seitenanzahl hinausgehen, werden nicht bewertet. <u>Bewertungsskala (durchgängig von 0 bis 4 BP):</u> • <u>0 BP</u>: Die Ausführungen fehlen, die Darstellung der genannten Risiken ist unzureichend oder die Lösungsansätze für identifizierte Risiken sind nicht vorhanden oder undifferenziert. • <u>1 BP</u>: Es wurde eine Risikoanalyse durchgeführt. Die Darstellung der genannten Risiken ist plausibel. Geeignete Lösungsansätze für identifizierte Risiken sind vorhanden, aber wenig differenziert. • <u>4 BP</u>: Es wurde eine Risikoanalyse durchgeführt. Die Darstellung der genannten Risiken ist fundiert. Geeignete Lösungsansätze für identifizierte Risiken sind vorhanden und differenziert.	1	1	1	4
2	A/B	KG 2: Projektorganisation und Kosten			2	8
2.1	B	<u>Personalprofile und Rollen</u> Erstellen Sie von sämtlichen Personen des angebotenen Projektteams ein Personalprofil. Mindestens die Projektleitung (PL) sowie die stellvertretende Projektleitung (sPL) sind namentlich zu benennen. Geben Sie im Profil der PL auch die Kontaktdaten (E-Mail, Telefon) an.	1	2	2	8

Nr.	Kriterien- art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		Zulässig sind ausschließlich Personalprofile von real existierenden Personen. Diese müssen im Falle der Auftragsausführung verbindlich für das Projekt zur Verfügung stehen (vgl. Kapitel 4.1.3). Stellenprofile ohne bereits hinterlegtes Personal sind unzulässig. Ordnen Sie die einzelnen Personen den beteiligten Unternehmen (Anbieter / Mitglieder der Bietergemeinschaft / Unterauftragnehmer) zu. Erläutern Sie in den Personalprofilen die Kenntnisse und Erfahrungen der einzelnen Personen anhand ihrer Bildungsabschlüsse und/oder anhand von konkreten Projekten / Aufträgen / Publikationen, an denen die einzelnen Personen maßgeblich beteiligt waren. Gehen Sie dabei explizit auf den fachlichen Schwerpunkt dieser Projekte / Aufträge / Publikationen ein (Verweis auf bei den Eignungskriterien aufgeführte Referenzen der beteiligten Unternehmen möglich) und erläutern Sie die Tätigkeiten, die von der jeweiligen Person im Rahmen dieser Projekte / Aufträge / Publikationen erbracht wurden und welche Erfahrungen die jeweilige Person dabei sammeln konnte, die für das hier zu vergebende Projekt / die Abdeckung der definierten Mindestanforderungen relevant sind. Es muss für das BSI klar ersichtlich sein, welche konkreten Mindestanforderung aus Kapitel 4.1.2 mit den beschriebenen Projekten / Aufträgen / Publikationen abgedeckt werden. Die hier genannten Projekte / Aufträge / Publikationen, an denen die hier angebotenen Personen des Projektteams maßgeblich beteiligt waren, müssen nicht mit dem derzeitigen Arbeitgeber (Bieter / Mitglied der Bietergemeinschaft / Unterauftragnehmer) im Zusammenhang stehen. Die gesamte Darstellung sollte pro Person zwei DIN-A4 Seiten nicht überschreiten. Ordnen Sie zudem in einer tabellarischen Übersicht die angebotenen Personen / die Personalprofile konkreten Rollen / Tätigkeiten im Sinn von Projektleitung, Entwickler, Techniker, wissenschaftlicher Mitarbeiter, technischer Berater, etc. zu. Anmerkung: die im vorherigen Satz vom BSI exemplarisch genannten Rollen dienen lediglich der Anschauung und wurden nicht auf das hier zu vergebende Projekt abgestimmt. Erwartungshorizont:				

Nr.	Kriterien- art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		Die Erfüllung der Mindestanforderungen gem. Kapitel 4.1.2 wird nachvollziehbar dargestellt (A-Kriterium). Über die Mindestanforderungen hinausgehend (B-Kriterium): Mindestens eine Person des Projektteams verfügt über weit reichende Kenntnisse in der CC-Zertifizierung. Die Projektleitung verfügt über vertiefte fachliche Kenntnisse in der sicheren Softwareentwicklung. Mindestens zwei Personen des Projektteams verfügen über wissenschaftliche Publikationen innerhalb der letzten zwei Jahre im Bereich der ausgeschriebenen Leistung und befassen sich regelmäßig mit aktuellen Veröffentlichungen im KI-Bereich oder im Bereich der sicheren Softwareentwicklung. <u>Bewertungsskala (durchgängig von 0 bis 4 BP):</u> • <u>0 BP:</u> Das Personalprofil erfüllt keinen Aspekt des Erwartungshorizontes. • <u>1 BP:</u> Das Personalprofil erfüllt die Mindestanforderungen. • <u>4 BP:</u> Das Personalprofil erfüllt die Mindestanforderungen, und darüber hinaus in vollem Umfang die Anforderungen des Erwartungshorizontes.				
2.2	A	<u>Kalkulation der Festpreise</u> Stellen Sie für jedes einzelne AP, welches nach Festpreis vergütet wird (siehe Kapitel 3.1 und 3.2), Ihre Kostenkalkulation dar. <u>Mindestanforderung:</u> Das Angebot enthält eine tabellarische Übersicht, aus der für jedes einzelne AP, welches gemäß Kapitel 3.1 und 3.2 nach Festpreis vergütet wird, die folgenden Angaben entnommen werden können: • An der Durchführung des jeweiligen AP beteiligte Personen / Rollen (siehe Zuschlagskriterium 2.1 „Personalprofile und Rollen“) • Tagessätze (zzgl. USt.) der jeweiligen Personen / Rollen (inkl. Gemeinkosten, etc.) • Kalkulierte Personentage pro Person / Rolle • Die aus den zuvor angegebenen Tagessätzen und kalkulierten Personentagen resultierenden Personalkosten • Ggf. anfallende Material- und Lizenzkosten. Setzen sich diese aus mehreren größeren	-	-	-	-

Nr.	Kriterien-art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		Einzelpositionen zusammen, so sind diese in einer separaten Tabelle aufzuschlüsseln. Höhe der Festpreise (zzgl. USt.) der einzelnen AP (resultierend aus den aufgeführten Personal-, Reise- und Materialkosten). Die bei den einzelnen AP vorgesehenen Personen / Rollen sowie die jeweils veranschlagten Personentage erscheinen unter Berücksichtigung der sonstigen Ausführungen im Angebot plausibel und stehen nicht im Widerspruch zu den in Kapitel 4.1.2 geforderten Mindestqualifikationen des für die Leistungserbringung einzusetzenden Personals.				
2.3	A	<u>Kalkulation der maximalen Obergrenzen</u> Stellen Sie für jedes einzelne AP, welches nach Aufwand vergütet wird (siehe Kapitel 3.1 und 3.2), Ihre Kalkulation der angebotenen Obergrenze dar. <u>Mindestanforderung:</u> Das Angebot enthält eine tabellarische Übersicht, aus der für jedes einzelne AP, welches gemäß Kapitel 3.1 und 3.2 nach Aufwand vergütet wird, die folgenden Angaben entnommen werden können: - An der Durchführung des jeweiligen AP beteiligte Personen / Rollen (siehe Zuschlagskriterium „Personalprofile und Rollen“) - Der einheitlicher Tagessatz (zzgl. USt.) für sämtliche Personen / Rollen; der Tagessatz muss in allen AP, welche nach Aufwand vergütet werden, identisch sein. Gemeinkosten, Materialkosten sowie sonstige Kosten (mit Ausnahme etwaiger Lizenzkosten gem. Kapitel 3.1.2.2) werden <u>nicht</u> gesondert vergütet und müssen daher bereits in den veranschlagten Tagessätzen enthalten sein. Es ist davon auszugehen, dass Reisen im Projekt nicht erforderlich sind. - Kalkulierte Personentage (PT) pro Person / Rolle <u>Achtung:</u> Bei AP 2, 3, 5, 6 und 7 wurde vom BSI jeweils ein Kontingent von PT festgelegt, d.h. die Summe der kalkulierten Personentage muss diesen Kontingenten jeweils <u>genau</u> entsprechen. - Höhe der jeweiligen maximalen Obergrenzen (zzgl. USt.) der einzelnen AP (resultierend aus den aufgeführten Tagessätzen und Personentagen) Die bei den einzelnen AP vorgesehenen Personen / Rollen sowie die jeweils veranschlagten Personentage erscheinen unter Berücksichtigung der sonstigen	-	-	-	

Nr.	Kriterien-art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		Ausführungen im Angebot plausibel und stehen nicht im Widerspruch zu den in Kapitel 4.1.2 geforderten Mindestqualifikationen des für die Leistungserbringung einzusetzenden Personals.				
2.4	A	<u>Zahlungs- und Meilensteinplan</u> Erstellen Sie anhand der Vorgaben in Kapitel 3.1 und 3.2 einen verbindlichen Zahlungs- und Meilensteinplan in tabellarischer Form mit folgenden Spalten (analog zur Darstellung in Tabelle 1 in Kapitel 3.2): • Arbeitspaket / Meilenstein • (Kurz-) Bezeichnung • Beginn • Ende • Art der Vergütung Die verbindlichen Vorgaben des AG (z.B. Art der Vergütung) sind dabei zwingend zu beachten. Weiterhin ist zu berücksichtigen, dass vor Durchführung eines optionalen Arbeitspakets eine gewisse Zeit für die Beauftragung des entsprechenden Arbeitspakets benötigt wird. Dies muss bei der Zeitplanung einkalkuliert werden. Stellen Sie den Ablauf des Projektes <u>zudem</u> als Gantt-Diagramm dar. Die zeitliche Planung ist im Angebot unter der Annahme zu erstellen, dass die Auftragserteilung erst unmittelbar vor Ablauf der Bindefrist des Angebotes erfolgt. Bei der späteren Leistungserbringung sind sämtliche in Kapitel 3.2 definierten verbindlichen zeitlichen Vorgaben (inkl. „maximaler zeitlicher Abstand zwischen Auftragserteilung und Projektstart“ sowie „maximale Projektlaufzeit“) jedoch auch dann einzuhalten, wenn das Vergabeverfahren früher als geplant erfolgreich abgeschlossen werden kann. In diesem Fall ist die zeitliche Planung des erfolgreichen Bieters in Abstimmung mit dem BSI entsprechend anzupassen (vgl. Kapitel 2.1). Die Dauer der einzelnen AP kann von jedem Bieter individuell kalkuliert werden, d.h. Abweichungen von den unverbindlichen Schätzwerten des AG (siehe Kapitel 3.2, Tabelle 1, Spalte „Termin nach Projektstart [Kalendermonate], Beginn, Ende“) sind durchaus möglich. <u>Mindestanforderung:</u> • Der Meilensteinplan bildet alle AP / Leistungen, die in Kapitel 3.2, Tabelle 1 dargestellt sind, ab.	-	-	-	-

Nr.	Kriterien- art	Kriteriengruppe (KG) / Kriterien	BP _{min}	GF	LP _{min}	LP _{max}
		Enthält Kapitel 3.2 verbindliche Vorgaben bzgl. der Bearbeitungsreihenfolge der einzelnen AP / Leistungen, so wurden diese eingehalten. - Wurde die Reihenfolge einzelner AP in Kapitel 3.2 nicht verbindlich vorgegeben und weicht die im Angebot enthaltene Planung bei diesen AP / Leistungen von der in Kapitel 3.2, Tabelle 1 dargestellten Reihenfolge ab, so wurde diese Abweichung detailliert begründet. Die abweichende Planung erscheint aus Sicht des BSI zweckmäßig. - Im Angebot ist jeweils ein konkretes Datum für die Fertigstellung der einzelnen Arbeitspakete sowie für das Erreichen der einzelnen Meilensteine angegeben. Diese erscheinen aus Sicht des BSI realistisch und plausibel. - Die verbindlichen zeitlichen Vorgaben aus Kapitel 3.2 (z.B. maximaler Zeitrahmen für die Leistungserbringung) wurden eingehalten. - Wurde die in Kapitel 3.2, Tabelle 1 dargestellte Meilensteinplanung zwecks Einführung zusätzlicher Zahlungszeitpunkte um weitere Meilensteine ergänzt, so wurden dabei die in Kapitel 3.2 definierten Vorgaben bzgl. Abnahmefähigkeit der Leistungen und Zulässigkeit der Rechnungslegung beachtet.				
Gesamt:				11	11	44

6.2.2 Anlage: Bietergemeinschaftserklärung

Wird das Angebot von einer Bietergemeinschaft abgegeben, so ist dem Angebot eine entsprechende Erklärung beizufügen (siehe standardisiertes Formular in den Vergabeunterlagen). Diese Erklärung ist von allen Mitgliedern der Bietergemeinschaft zu signieren (siehe Ziffern 3.4.2 und Ziffer 6.2 der Allgemeinen Bewerbungsbedingungen).

6.2.3 Anlage: Unterauftragnehmerverspflichtungserklärung(en)

Sollen wesentliche Teile der angebotenen Leistung von einem oder mehreren Unterauftragnehmern für den Bieter erbracht werden, so ist dem Angebot pro Unterauftragnehmer eine entsprechende Verpflichtungserklärung beizufügen (siehe standardisiertes Formular in den Vergabeunterlagen). Diese sind von den Unterauftragnehmern zu signieren (siehe Ziffern 3.4.2 und Ziffer 6.3 der Allgemeinen Bewerbungsbedingungen).

6.2.4 Anlage: Angaben zu vorliegenden Ausschlussgründen und zur Selbstreinigung im Sinne von § 125 GWB

Liegt mindestens ein zwingender oder fakultativer gesetzlicher Ausschlussgrund bei dem Bieter, bei einem Mitglied der Bietergemeinschaft oder bei einem Unterauftragnehmer vor (siehe Kapitel 5.1), so ist dem Angebot eine entsprechende Erklärung als Anlage beizufügen. Diese muss mindestens die folgenden Angaben enthalten:

- Abschließende Auflistung aller vorliegenden Ausschlussgründe im Sinne von den § 123 und § 124 GWB
- Detaillierte Erläuterungen zu den vorliegenden Ausschlussgründen. Insbesondere enthalten die Erläuterungen Angaben zur Art der Straftat, zur Höhe des fraglichen Betrages, zum Datum einer rechtskräftigen Gerichtsentscheidung / bestandskräftigen Verwaltungsentscheidung, zur Dauer des festgelegten Ausschlusszeitraums sowie zu den eingegangenen Verpflichtungen im Sinne von § 123 Abs. 4 Satz 2 GWB.
- Betroffene Maßnahmen zur Selbstreinigung im Sinne von § 125 GWB.

Die Anlage ist zu signieren (siehe Ziffern 3.4.2 der Allgemeinen Bewerbungsbedingungen).

C Abkürzungsverzeichnis⁵

AG	Auftraggeber
AN	Auftragnehmer
AP	Arbeitspaket
AVA	Assurance Class: Vulnerability Assessment in der Common Criteria Bewertung
BMWi	Bundesministerium für Wirtschaft und Energie
BP	Bewertungspunkte
BP _{min}	Mindestpunktzahl (Bewertungspunkte)
BQM	Beauftragte/Beauftragter für Qualitätsmanagement
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
GP	Gewichtungspunkte
KG	Kriteriengruppe
KI	Künstliche Intelligenz
LP	Leistungspunkte
LP _{max}	Maximalpunktzahl (Leistungspunkte)
LP _{min}	Mindestpunktzahl (Leistungspunkte)
MS	Meilenstein
PDF	Portable Document Format
PL	Projektleitung
PoC	Proof of Concept
sPL	stellvertretende Projektleitung
SSDLC	Secure Software Development Life Cycle
SÜG	Sicherheitsüberprüfungsgesetz
Ü2	Erweiterte Sicherheitsüberprüfung
VS-NfD	Verschlusssache – Nur für den Dienstgebrauch

⁵ Das Abkürzungsverzeichnis erhebt keinen Anspruch auf Vollständigkeit. Auch kann dieses standardisierte Verzeichnis ggf. Abkürzungen und Begriffe zu inhaltlichen Punkten enthalten, die nicht Gegenstand der hier vorliegenden Leistungsbeschreibung sind (z.B. SÜG).

D Muster Leistungsnachweis

Im Folgenden finden Sie ein Beispiel für den Aufbau eines Leistungsnachweises und welche Informationen dieser erhalten sollte. Auf Wunsch wird das Muster als elektronisches Dokument nach Auftragsvergabe von der Projektleitung zur Verfügung gestellt.

Hinweis: Leistungsnachweise müssen ausschließlich bei Vergütung nach Aufwand mit der Rechnung eingereicht werden.

Leistungsnachweis für Auftrag [AUFTRAGSNUMMER] (Projekt XY)

Erstellungsdatum xx.xx.xxxx

Lfd.Nr.	Datum Leistungserbringung	Mitarbeiter Kategorie ^{*2}	Mitarbeiter des AN	Arbeitspaket-Nr. gemäß Leistungsbeschreibung	Beschreibung Tätigkeit (kurze Beschreibung der ausgeführten/erbrachten Leistungen)	Personentage ^{*1}	Tagessatz (inkl. Ust.) gemäß Angebot	Einzelpreis (Personentage X Tagessatz)
1			Name, Vorname		Beratung zu Thema xx			0,00 €
2			Name, Vorname		Bearbeitung Dokument xx			0,00 €
3			Name, Vorname		etc. pp.			0,00 €
4			Name, Vorname					0,00 €
5			Name, Vorname					0,00 €
6			Name, Vorname					0,00 €
7			Name, Vorname					0,00 €
8			Name, Vorname					0,00 €
9			Name, Vorname					0,00 €
10			Name, Vorname					0,00 €
11			Name, Vorname					0,00 €
						Gesamtaufwand in Tagen (oder andere Einheit gemäß Vertrag)	Durchschnittlicher Tagessatz	Gesamtpreis
						0	#DIV/0!	0,00 €

^{*1} acht Zeitstunden ergeben einen Personentag. Wurden weniger als acht Zeitstunden pro Tag geleistet, sind diese anteilig (viertelstundengenau) anzugeben.

^{*2} z.B. PL = Projektleiter*In, PA = Projektassistenz