

0.1 EU_ Formular für Bewerberfragen

Projekt-/Maßnahme:

System zur Angriffserkennung

(Vergabe-)Leistungsgegenstand:

Beschaffung eines Systems zu Angriffserkennung SIEM/VMS

eVergabe-Nr.:

CXRAY6YYHW5

Auftraggeber:

Flughafen Stuttgart GmbH (FSG)

Lfd. Nr.	Bewerberfrage	Datum	Stellungnahme FSG	Datum
1	Wir bitten um Klarstellung und Anpassung der Vertraulichkeitsvereinbarung auf den marktüblichen Standard in Bezug auf den Umfang und Zeitraum des Informationsschutzes. Nach vorliegendem Dokument soll sich der Schutz auch auf Informationen beziehen, die ggf. bereits in der Vergangenheit durch den Auftragnehmer erhalten wurden. Marktüblich sind Vertraulichkeitsregelungen, die sich auf den gegenwärtigen und zukünftigen Austausch von vertraulichen Informationen beziehen.	22.01.2026	Bitte haben Sie Verständnis dafür, dass wir von unserer bestehenden Standard-Geheimhaltungsvereinbarung ("16_Geheimhaltungsvereinbarung") nicht abweichen werden. Diese gilt für alle Bewerber dieses Verfahrens einheitlich und stellt sicher, dass sowohl bereits im Rahmen einer bestehenden Geschäftsbeziehung ausgetauschte Informationen als auch zukünftige vertrauliche Inhalte angemessen geschützt werden. Aus unserer Sicht ist es wesentlich, dass sämtliche im Zusammenhang mit der Zusammenarbeit stehenden Informationen, unabhängig vom Zeitpunkt ihrer Weitergabe, dem gleichen Vertraulichkeitsstandard unterliegen. Daher können wir die beantragte Einschränkung auf ausschließlich gegenwärtige und zukünftige Informationen nicht vornehmen.	28.01.2026
2	Kann der Nachweis zur Erfüllung der Anforderung "Nachweis eines dokumentierten Qualitätsmanagements (z. B. ISO 9001 oder vergleichbar)" durch eine Eigenerklärung erbracht werden, da die Anforderung ja ein dokumentiertes und kein zertifiziertes Qualitätsmanagement verlangt?	22.01.2026	Die Vergabeunterlagen sehen einen qualifizierten Nachweis über ein Qualitätsmanagementsystem vor. Dieser Nachweis kann nicht allein durch eine Eigenerklärung erbracht werden. Er ist durch die Vorlage entsprechender Zertifikatsunterlagen oder eines gleichwertigen, unabhängigen Nachweises zu führen. Dies ergibt sich aus dem Teilnahmeantrag, in dem ausdrücklich festgelegt ist, dass „der Bewerber nachzuweisen hat, dass eine anerkannte Zertifizierung im Bereich Qualitätsmanagement oder ein vergleichbarer Nachweis vorliegt. Der Nachweis ist durch Vorlage entsprechender Zertifikatsunterlagen zu erbringen.“ Das Ankreuzen der Passage „Der Anbieter kann eine Zertifizierung nach ISO 9001 oder ein vergleichbares Zertifikat vorweisen.“ stellt die Eigenerklärung bereits dar. Ergänzend ist jedoch die Einreichung des Zertifikats (oder eines gleichwertigen unabhängigen Nachweises) als Anlage zwingend erforderlich. Eine reine Selbstauskunft genügt daher nicht.	28.01.2026

3	Darf die Leistungserbringung der Services aus Europa oder muss diese zwingend aus DACH erfolgen?	02.02.2026	Die Leistungserbringung der Services kann aus Europa erfolgen, sollte allerdings deutschsprachig sein. Bitte nehmen Sie zur Kenntnis, dass wir eine konkretere Auskunft dazu in der aktuellen Phase nicht abfragen und erst im Rahmen der Phase 2 (Aufforderung zur Angebotseinholung) relevant wird.	03.02.2026
4	Im Falle einer Angebotsabgabe, die auf einer virtuellen Lösung basiert, welche in der bestehenden FSG-Infrastruktur betrieben wird (gemäß Ziffer 1.1.5, Punkt 2. der Leistungsbeschreibung), bitten wir um Klärung, ob die Kosten für die hierfür benötigten virtuellen Maschinen (VMs) – insbesondere in Bezug auf die Lizenzierung (z.B. VMware ESXi, Hyper-V) und die Bereitstellung der notwendigen Ressourcen (Speicher, Virtualisierungsumgebung, Backup) – vom Auftraggeber (FSG) direkt getragen werden und somit nicht durch den Auftragnehmer bepreist werden müssen.	02.02.2026	Die Kosten für die Bereitstellung der notwendigen infrastrukturellen Ressourcen werden vom Auftraggeber getragen und müssen nicht eingepreist werden. Hinweis: Die Frage bezieht sich bereits auf die Angebotsphase und wird erst in der Phase 2 (Aufforderung zur Angebotsabgabe) relevant.	03.02.2026
5	Die aktuell ermittelten Systemkomponenten für das Vulnerability Management System (VMS) umfassen Tenable One, Tenable Nessus, Tenable Agent und Tenable OT/Identity Exposure. Wir bitten um eine verbindliche Klärung, ob die Kosten für die genannten Lizenzen des VMS (Tenable-Produkte) für die gesamte Vertragslaufzeit vom Auftraggeber (FSG) gestellt und getragen werden oder ob diese Kosten vom Auftragnehmer zu kalkulieren und im Managed Service Vertrag zu berücksichtigen sind.	02.02.2026	Es handelt sich hierbei um die aktuell ermittelten Systemkomponenten. Wir stellen für die neue Vertragslaufzeit keine Lizenzen für das Vulnerability Management zur Verfügung. Wir erwarten ein Komplettangebot bestehend aus Managed Service und entsprechender Lizenzierung (in der Phase 2). Hinweis: Die Frage bezieht sich bereits auf die Angebotsphase und wird erst in der Phase 2 (Aufforderung zur Angebotsabgabe) relevant.	03.02.2026
6	Um eine realistische Kalkulation des Managed Service, insbesondere der Leistungsparameter für Detection & Response, zu ermöglichen, bitten wir um folgende ergänzende Informationen: Wie viele Use Cases müssen vom Auftragnehmer (AN) im Rahmen der Systemübernahme übernommen werden? Für welche Systeme sind die Use Cases implementiert? Kann in der nächsten Phase der Ausschreibung eine Liste der Use Cases bereitgestellt werden? Welche durchschnittliche tägliche oder monatliche Anzahl von Vorfällen bzw. Alarmen generiert das System zur Angriffserkennung (SzA) derzeit, aufgeschlüsselt nach den definierten Vorfällen (High, Medium, Low)?	02.02.2026	Mit den Bewerbern, welche die Aufforderung zur Angebotsabgabe erhalten werden (Phase 2), tauschen wir nach Unterzeichnung einer Geheimhaltungsvereinbarung die Use Cases aus. Wie bereits im Teilnahmeantrag Kapitel X. Nr. 5 ist eine unterzeichnete Geheimhaltungsvereinbarung Voraussetzung für die Einladung zur Phase 2 (Aufforderung zur Angebotsabgabe) sowie für den Erhalt der Use Cases.	03.02.2026
7	In Ziffer 2.2.2 der Leistungsbeschreibung wird gefordert, dass der Anbieter nur Personal einsetzt, welches einer Zuverlässigkeitsüberprüfung gemäß §7 Luftsicherheitsgesetz (LuftSiG) unterzogen wurde. Wir bitten um Klärung, ob diese Anforderung: ausschließlich für Personal gilt, das physische Präsenz am Flughafen Stuttgart (Leistungsort) erbringt (Vor-Ort-Leistungen), oder auch für Personal gilt, das die Leistung remote erbringt und lediglich über einen VPN-Tunnel auf das System zur Angriffserkennung (SzA) zugreift.	02.02.2026	Dies gilt für das gesamte zur Leistungserbringung eingesetzte Personal.	03.02.2026

8	<p>Die vom Auftraggeber verlangte Haftpflichtversicherung ist deutlich höher als im vergleichbaren Leistungsumfeld üblich. Bei der Haftpflichtversicherung handelt es sich um eine Eignungsanforderung zur wirtschaftlichen / finanziellen Leistungsfähigkeit. Diese muss dem Wirtschaftlichkeits- und Verhältnismäßigkeits-Grundsatz entsprechen (vgl. § 97 Abs. 1 GWB, § 45 Abs. 1 Nr. 3 VgV). Die angeforderte Haftpflichtversicherung muss hierbei erforderlich und angemessen sein und sich am konkreten Risiko des Auftrags orientieren. Die hiesige Forderung (Versicherungsumfang von 20 Mio. EUR je für Personen-/Sachschäden und für Vermögensschäden, je zweifach maximiert pro Kalenderjahr) ist vor diesem Hintergrund zu hoch. Ist die Anforderung überhöht, werden überdies kleinere und mittlere Bieter vom Wettbewerb ausgeschlossen, da diese einen solchen Versicherungsschutz kaum wirtschaftlich erlangen werden.</p> <p>Wir bitten daher um Anpassung der Versicherungs-Anforderung auf den marktüblichen Standard (d.h. nicht mehr als 10 Mio. EUR für Personen-/Sach- bzw. Vermögensschäden; Deckung 2-fach pro Kalenderjahr, Umweltschäden einfach).</p>	02.02.2026	<p>Die angesetzten Mindestdeckungssummen orientieren sich bewusst am konkreten Risikoprofil des Auftrags, insbesondere an möglichen Cyber- und Systemausfallrisiken mit KRITIS-Bezug. Ein durch Fehlfunktionen des Systems verursachter Ausfall zentraler IT-Infrastrukturen kann im Luftverkehrsbetrieb zu betriebsweiten Unterbrechungen, erheblichen Umsatzausfällen sowie umfangreichen Regressforderungen (z. B. seitens Airlines) führen. Das potenzielle Schadensvolumen liegt damit deutlich über dem in gewöhnlichen IT-Leistungsszenarien üblichen Rahmen.</p> <p>Die Anforderungen sind risikobasiert, nicht überhöht und notwendig, um das reale Schadenspotenzial abzudecken. Vor diesem Hintergrund erachten wir die festgelegten Mindestversicherungssummen weiterhin für angebracht, sachgerecht und marktüblich, weshalb von einer Anpassung abgesehen wird.</p>	05.02.2026
9	<p>Wir bitten um Klärung bezüglich des Vulnerability Managements (VMS). Gehen wir richtig in der Annahme, dass für das Vulnerability Management seitens der FSG keine Schwachstellenanalyse (Vulnerability Analyse) erwartet wird, sondern lediglich die Unterstützung bei Fragen durch den AG sowie ein Updateservice der lokalen Scankomponenten (Tool Management), wie in Abschnitt 4.5.4 beschrieben?</p>	03.02.2026	Ihre Annahme ist korrekt.	05.02.2026
10	<p>Wir bitten um Klärung der Installationsanforderungen für die VMS-Scannerinfrastruktur. Gehen wir richtig in der Annahme, dass sämtliche Scanner in virtuellen Maschinen installiert werden können (gemäß Abschnitt 1.1.6) und keine isolierten Systeme (Air-Gapped) vorhanden sind, sodass der VMS-Service vollständig remote erbracht werden kann?"</p>	03.02.2026	Es sind keine Air-Gapped Scanner vorhanden. Die Installation der Scankomponenten erfolgt überwiegend in virtuellen Maschinen. Die eingesetzten Hardwaresensoren sind an das Management System angebunden. Somit kann der Service remote erbracht werden.	05.02.2026
11	<p>Wir unterliegen zwingenden gesetzlichen Bestimmungen des Berufsrechts sowie einer Berufsaufsicht. Unsere Tätigkeiten sind nach § 43 Abs. 1 i.V.m. § 56 WPO unabhängig, gewissenhaft, verschwiegen und eigenverantwortlich auszuüben.</p> <p>In den Ausschreibungsunterlagen sind an folgenden Stellen Prüfrechte des Auftraggebers enthalten:</p> <p>Dokument Klausel Kerninhalt EVB-IT Cloud-AGB: Ziffer 6.4 (insbes. 6.4.1, 6.4.2, 6.4.3), Nachweis IT-Sicherheit, Zugang zu Systemen, 12-Monats-Turnus</p> <p>EVB-IT Cloudvertrag Muster : Ziffer 8.3, Erweiterung auf BSI und Aufsichtsorgane</p> <p>AVV (Art. 28 DS-GVO): § 6 Abs. 5, § 7, Prüfrechte auch bei Unterauftragnehmern</p> <p>Leistungsbeschreibung: Ziffer 6.1.8, Recht auf Auditierung des Gesamtsystems</p> <p>ISMS-Richtlinie: Ziffer 8, Vor-Ort-Audits DSMS-Richtlinie Ziffer VI Vor-Ort-Audits, Zutritts-/Einsichtsrechte Dürfen wir davon ausgehen, dass die in den aufgeführten Textstellen normierten Auditrechte des Auftraggebers in Geschäftsräumen und Systemen des</p>		Noch in Klärung, Beantwortung folgt in Kürze	tbd

	Auftragnehmers grundsätzlich nur insoweit Anwendung finden, als dass diese nicht im Widerspruch zu den berufsrechtlichen Verschwiegenheitspflichten und sonstigen gesetzlichen Pflichten des Auftragnehmers stehen und nur im Rahmen des berufsrechtlich Möglichen und Zulässigen ausgeübt werden	04.02.2026		
12	Müssen eingesetzte Subunternehmer zwingend nach ISO 27001 und ISO 9001 zertifiziert sein?	05.02.2026	Noch in Klärung, Beantwortung folgt in Kürze	tbd