

BESCHAFFER-GUIDE

Zwölf Fragen an einen Softwarelieferanten für sicherheitskritische Systeme.

Ein Prüfleitfaden für Beschaffer, Programm-Manager und Fachverantwortliche in Aerospace, Defence, Automotive und kritischen Infrastrukturen.

AUSGABE	UMFANG	BAUSTEIN	ABSENDER
1 / 2026	12 Prüfpunkte	01 von 06	new direction GmbH

Softwareprojekte in sicherheitskritischen Umgebungen folgen einer anderen Logik als die tägliche Business-IT. Ein Fehler im Code lässt sich nicht durch einen unbemerkten Hotfix am nächsten Tag beheben. Er berührt Verfügbarkeit im Einsatz, Verantwortung im Betrieb und, bei staatlichen Fachanwendungen, den Bestand einer Verwaltungsleistung.

Die folgenden zwölf Fragen unterstützen Sie dabei, in einem Erstgespräch oder in einer Angebotsprüfung schnell zu erkennen, ob ein Lieferant tatsächlich beschafferfähig ist. Zwei der Fragen (elf und zwölf) betreffen Aspekte, die in Standard-Prüfkatalogen selten vorkommen, sich in der Praxis aber als hochrelevant erwiesen haben.

Jede Frage folgt derselben Struktur. Eine Kernaussage, ein Prüfhinweis, ein Kontext, ein Antwortmuster mit Substanz, ein Warnzeichen, und eine kurze Angabe zur eigenen Position von new direction. Sie können den Guide unverändert nutzen, an interne Prüfprozesse anpassen oder als Grundlage für eine schriftliche Lieferantenbefragung einsetzen.

01 Zertifizierungen im gelebten Alltag

PRÜFT: OB ZERTIFIKATE IM ENTWICKLUNGSALLTAG TATSÄCHLICH ANGEWENDET WERDEN.

Welche Zertifizierungen liegen vor, wann wurde zuletzt auditiert, und wie werden die zugehörigen Prozesse in Ihrem Entwicklungsalltag angewendet? Eine ISO 9001 reicht im sicherheitskritischen Umfeld selten aus. Relevant ist der Nachweis, dass Prozesse standardisiert und geprüft sind und dass Entwickler die Vorgaben selbst erklären können.

ANTWORT MIT SUBSTANZ

Aktuelle TISAX-Auditierung mit hohem Schutzbedarf, EcoVadis Gold oder vergleichbare Bewertung, konkrete Prüfdaten mit Ablaufhorizont, sichtbare Umsetzung in CI/CD-Pipelines und Freigabepfaden.

WARNZEICHEN

Zertifikate erscheinen dauerhaft "in Planung", Auditdaten fehlen, Entwickler kennen die zugrundeliegenden Anforderungen nicht.

NEW DIRECTION DAZU: TISAX-Auditierung 2025 bestanden, gültig bis 2028. EcoVadis Gold aktuell. ISO 27001 in Vorbereitung. Alle Entwickler durchlaufen ein achttündiges Sicherheits- und Prozess-Onboarding.

PRÜFT: DIE RÄUMLICHE UND PERSONELLE ZUGANGSBARRIERE ZU KLASSIFIZIERTEN INFORMATIONEN.

Ist Ihr Standort sicherheitsüberprüft, und wie viele Mitarbeitende sind zum aktuellen Zeitpunkt sicherheitsüberprüft? Für Aufträge im Verteidigungs-, Behörden- und Dual-Use-Kontext ist die räumliche und personelle Zugangsbarriere Voraussetzung, nicht Zusatz.

ANTWORT MIT SUBSTANZ

Sicherheitsüberprüfter Standort im Inland, Personal mit definiertem Prüfstatus, Onshore-Entwicklung, klare Aussage zur Zahl geprüfter Personen mit Datum.

WARNZEICHEN

Ausweichende Antworten zu Subunternehmern, verteilte Entwicklung in unklaren Rechtsräumen, Zahlen ohne Zeitbezug.

NEW DIRECTION DAZU: Sicherheitsüberprüfter Standort in Augsburg. Anteil sicherheitsüberprüften Personals im Rahmen laufender Mandate, Ausweitung in Vorbereitung. Reine Onshore-Entwicklung ohne Offshore-Anteile.

PRÜFT: OB DER ANBIETER DEN EIGENEN STATUS PRO STANDARD EHRlich BENENNEN KANN.

Nach welchen domänenspezifischen Standards arbeiten Sie (etwa DO-178C, EMAR, STANAG 4586, ISO 26262, Automotive SPICE), und wie ehrlich benennen Sie den eigenen Status pro Standard? Zulassung und Beschaffungsfähigkeit hängen weniger davon ab, dass ein Anbieter Standards kennt, als davon, dass er die Nachweise (Traceability, Testabdeckung, Dokumentation) tatsächlich liefern kann.

ANTWORT MIT SUBSTANZ

Klare Unterscheidung zwischen "zertifiziert", "erfahren in", "orientiert an" und "in Vorbereitung". Verweise auf konkrete Vorgängerprojekte, in denen die Nachweise geliefert wurden.

WARNZEICHEN

Standards werden pauschal aufgezählt, ohne dass der Anbieter den eigenen Status pro Standard benennen kann.

NEW DIRECTION DAZU: Unsere Standards-Landkarte (Baustein 06 dieser Bibliothek) benennt für jeden Standard den tatsächlichen Status. TISAX zertifiziert. ISO 26262 und Automotive SPICE erfahren in. DO-178C, EMAR, STANAG 4586 orientiert an.

04 Referenzen mit vergleichbarer Kritikalität

PRÜFT: DIE ÜBERTRAGBARKEIT VORHANDENER ERFAHRUNG AUF DEN GEPLANTEN AUFTRAG.

Welche Referenzen aus vergleichbaren Kritikalitäts- und Regulierungsstufen können Sie benennen, und welche davon dürfen offen kommuniziert werden? Ein Anbieter mit ausschließlich zivilen Referenzen mag technisch fähig sein, ist aber ohne Erfahrung in Verwaltungsprozessen und Beschaffungslogik.

ANTWORT MIT SUBSTANZ

Konkrete Nennung von Kunden und Vertragsformen, klare Trennung zwischen offen zeigbaren und unter Geheimhaltung erwähnbaren Projekten, Übertragbarkeit auf Ihren Auftrag benennbar.

WARNZEICHEN

Referenzen bleiben vage, Namen werden pauschal geschwärzt, Kritikalitätsstufen werden nicht diskutiert.

NEW DIRECTION DAZU: Öffentlich: BMW EMV seit über 20 Jahren, TÜV Süd, GFAW STAR Systemübernahme, BM-DS Ground Control Station Ghost 150. Anonymisiert: .NET-Fachanwendungen einer nationalen Verteidigung 2024 bis 2028.

PRÜFT: OB DER ANBIETER IN PROJEKTLAUFZEITEN ODER IN LIFECYCLES DENKT.

Welche Vertragsmodelle bieten Sie für Wartung, Support und Change Requests an, und wie lange betreuen Sie Systeme in der Regel? Softwareverträge im staatlichen und wehrtechnischen Kontext laufen häufig vier bis acht Jahre und benötigen einen Partner, der über diese Zeitspanne stabil liefert.

ANTWORT MIT SUBSTANZ

Nachweisbare Kundenbeziehungen über zehn oder zwanzig Jahre, standardisierte Wartungsverträge, Change-Request-Prozesse mit dokumentierten Durchlaufzeiten, Obsoleszenz-Management als expliziter Bestandteil.

WARNZEICHEN

Der Anbieter denkt in Projekten, nicht in Lifecycles. Betreuung endet nach Projektabnahme. Change Requests werden ad hoc verhandelt.

NEW DIRECTION DAZU: Längste laufende Kundenbeziehung 25 Jahre. Wartungs- und Change-Request-Prozesse dokumentiert. Aktuelle Verträge im wehrtechnischen Bereich mit Vier-Jahres-Laufzeit.

PRÜFT: OB REAKTIONSZEITEN VERBINDLICH DEFINIERT ODER REIN ASPIRATIONAL SIND.

Innerhalb welcher Fristen antworten Sie auf Erstanfragen, wie hoch ist Ihre Reaktionsgarantie bei Störfällen, und über welche Kanäle kommunizieren Sie? Beschaffung im öffentlichen Sektor arbeitet mit klar definierten Reaktionszeiten. Ein Anbieter, der diese nicht offen benennen kann, wird in laufenden Verfahren schnell zum Engpass.

ANTWORT MIT SUBSTANZ

Zugesagte Erstantwort innerhalb weniger Werktage unter NDA, definierte Servicezeiten mit Personenerreichbarkeit, dedizierte E-Mail-Postfächer für Beschaffer, verschlüsselte Kommunikation auf Anfrage.

WARNZEICHEN

Reaktionszeiten werden nicht garantiert. Anfragen laufen über allgemeine Vertriebs-Postfächer. Verschlüsselte Kommunikation ist Marketing-Behauptung ohne technische Grundlage.

NEW DIRECTION DAZU: Zugesagte Erstantwort auf Beschaffer-Anfragen innerhalb von fünf Werktagen unter NDA. Dediziertes Postfach getintouchwith@newdirection.de. PGP auf Anfrage. Servicezeiten Mo bis Fr 08 bis 17 Uhr.

07 Sprachkompetenz und Behördenerfahrung

PRÜFT: DIE OPERATIVE SPRACHFÄHIGKEIT IM VERWALTUNGS- UND VERGABEKONTEXT.

Welche Sprachen deckt Ihr operatives Team ab, und welche vergaberechtlichen Prozesse beherrschen Sie? Reibungsverluste durch Sprachbarrieren oder Unkenntnis des Vergaberechts verlangsamen Beschaffungsprozesse erheblich und werden im Zuschlagsverfahren geprüft.

ANTWORT MIT SUBSTANZ

Muttersprachliche Abdeckung Deutsch und Englisch, für die Schweiz auch Französisch und Italienisch, direkte Erfahrung mit WTO-Vergaben, Selbstdeklaration BKB, Schweizer Beschaffungskonferenz.

WARNZEICHEN

Kommunikation nur über Vermittler oder externe Übersetzer. Erste Erfahrung mit Vergaberecht steht noch aus.

NEW DIRECTION DAZU: Deutsch, Englisch, Französisch operativ abgedeckt. Ständige Vertretung Schweiz in St. Gallen. Vergabeverfahren im WTO-Bereich zuletzt 2023 erfolgreich absolviert.

PRÜFT: OB DER ANBIETER DUAL-USE-PRÜFUNG ALS OPERATIVEN PROZESS FÜHRT.

Wie prüfen Sie Ihre Leistungen auf exportkontrollrechtliche Relevanz, und wie ist der interne Prozess bei Dual-Use-Klassifizierung organisiert?

Softwarekomponenten im Defence- und High-Tech-Umfeld können unter Verordnung (EU) 2021/821 und das Außenwirtschaftsgesetz fallen.

ANTWORT MIT SUBSTANZ

Etablierter interner Prüfprozess mit dokumentierter Zuständigkeit, klarer Umgang mit Drittanbieter-Libraries, Beschreibung der Entscheidungslogik bei Auftragsprüfung.

WARNZEICHEN

Unkenntnis über Dual-Use-Bestimmungen. Berufung auf externe Beratung ohne interne Verantwortung.

NEW DIRECTION DAZU: Interne Compliance-Verantwortung benannt. Jede Anfrage durchläuft eine Exportkontroll-Prüfung. Zuständiger Ansprechpartner: compliance@newdirection.de.

PRÜFT: DIE FÄHIGKEIT ZUR NAHTLOSEN FORTFÜHRUNG FREMDER CODEBASEN.

Haben Sie Erfahrung darin, ein laufendes System von einem Vorgängerdienstleister zu übernehmen, ohne den Betrieb zu unterbrechen? Selten startet ein Auftrag auf der grünen Wiese. Häufig geht es um die Fortführung eines Systems, das dokumentarisch oder personell dünn übergeben wird.

ANTWORT MIT SUBSTANZ

Standardisierter Übernahmeprozess, dokumentierte Referenzen für nahtlose Übergänge, Code-Audit- und Refactoring-Strategie ohne Betriebsunterbrechung.

WARNZEICHEN

Der Anbieter fordert pauschal den Neubau, weil die Einarbeitung in Fremdcode abgelehnt wird.

NEW DIRECTION DAZU: Zwei Systemübernahmen 2023 und 2024 erfolgreich abgeschlossen, davon eine im öffentlichen Sektor. Standardisierter Übernahmeprozess in vier Phasen dokumentiert (Baustein 05 dieser Bibliothek).

10 Eigentümerstruktur und Souveränität

PRÜFT: DIE EIGENTUMSRECHTLICHE KONTROLLE ÜBER QUELLCODE UND DATEN.

Wie ist die Eigentümerstruktur Ihres Unternehmens organisiert, und welche Kontrolle über Quellcode und Daten liegt tatsächlich in Ihrer Hand? Im wehrtechnischen und behördlichen Kontext prüfen Auftraggeber zunehmend die eigentumsrechtliche Souveränität ihrer Lieferanten.

ANTWORT MIT SUBSTANZ

Klare Auskunft zur Eigentümerstruktur, keine intransparenten Beteiligungen, Quellcode und Datenhaltung im Inland, keine Abhängigkeit von Zulieferern außerhalb des vereinbarten Rechtsraums.

WARNZEICHEN

Eigentümerstruktur wird bei Rückfragen ausweichend beantwortet. Quellcode oder Daten liegen in wechselnden Cloudregionen.

NEW DIRECTION DAZU: 100 Prozent deutsche Eigner. Keine ausländischen Beteiligungen. Quellcode-Repositories im Inland. Datenhaltung in geprüften deutschen Rechenzentren.

PRÜFT: WAS MIT IHREM SYSTEM PASSIERT, WENN IHR LIEFERANT ZAHLUNGSUNFÄHIG WIRD.

Beschaffungsverfahren betrachten selten die wirtschaftliche Fortbestandslage des Anbieters über die Vertragslaufzeit. Bei sicherheitskritischen Systemen mit langer Bindung kann eine unangekündigte Insolvenz zum Systemstillstand führen. Ein professioneller Anbieter hat für diesen Fall vorgesorgt und macht die Vorsorge transparent.

ANTWORT MIT SUBSTANZ

Quellcode-Escrow bei einem notariellen Hinterlegungsdienst, vertragliche Regelung zur Weitergabe der Rechte an den Auftraggeber im Insolvenzfall, dokumentierte Übergabe-Prozeduren, Absicherung der Betriebsfähigkeit für mindestens 90 Tage nach Insolvenzanmeldung.

WARNZEICHEN

Das Thema wird als unwahrscheinlich abgetan, keine Escrow-Regelung, keine dokumentierte Prozedur für den Insolvenzfall, keine belastbare Kapitalstruktur.

NEW DIRECTION DAZU: Escrow-Vereinbarungen mit notariellem Hinterlegungsdienst in Vorbereitung für alle langlaufenden Mandate. Dokumentierte Übergabe-Prozedur. Solide Eigenkapitalbasis. Fortbestand seit 1998.

PRÜFT: DIE GRAUZONE DER ZUGANGSKONTROLLE BEI WERKSTUDENTEN, PRAKTIKANTEN, EXTERNEN BERATERN.

Wie regeln Sie den Zugang von Werkstudentinnen, Praktikantinnen und externen Beratern zu Quellcode und Testdaten in Ihren Aufträgen? Die meisten Zertifizierungen regeln festes Personal. Befristete Kräfte und externe Berater sind oft in einer Grauzone. In sicherheitskritischen Projekten ist genau diese Grauzone das häufigste Einfallstor.

ANTWORT MIT SUBSTANZ

Klare Regelung zur Sicherheitsüberprüfung befristeter Kräfte, dokumentierte Zugriffsrechte je Rolle, technische Trennung sensibler Bereiche, automatisierte Löschung von Zugängen nach Vertragsende, Onboarding- und Offboarding-Prozeduren.

WARNZEICHEN

Werkstudenten haben pauschalen Repository-Zugriff, externe Berater arbeiten remote ohne kontrollierten Zugang, keine dokumentierten Prozeduren für Beendigung von Zugängen.

NEW DIRECTION DAZU: Werkstudenten und Praktikanten arbeiten ausschließlich in nicht-klassifizierten Projekten. Rollenbasierte Zugriffsrechte. Automatisierte Offboarding-Prozedur mit Zugangswiderruf am Tag des Ausscheidens.

ZUM WEITEREN AUSTAUSCH

Dieser Guide ist Teil unserer Beschaffer-Bibliothek.

Fünf weitere Dokumente stehen in derselben Bibliothek zum freien Download bereit. Für Rückfragen zu einzelnen Prüfpunkten oder zur Anwendung des Guides auf konkrete Beschaffungsverfahren sind wir unter getintouchwith@newdirection.de innerhalb von fünf Werktagen erreichbar. Auf Wunsch unter beidseitiger Geheimhaltung.

E-MAIL FÜR BESCHAFFER
getintouchwith@newdirection.de

VERTRETUNG SCHWEIZ
St. Gallen · +41 71 45522-57

