PROCUREMENT GUIDE

Twelve questions for a software supplier for safety-critical systems.

A guideline for procurement officers, program managers and subject matter experts in aerospace, defense, automotive and critical infrastructures.

OUTPUT	SCOPE	BUILDING BLOCK	SENDER
1/2026	12 checkpoints	1 of 6	new direction GmbH

Software projects in security-critical environments follow a different logic than everyday business IT. A bug in the code cannot be fixed with an unnoticed hotfix the next day. It affects operational availability, responsibility in operation, and, in the case of government applications, the continued existence of an administrative service.

The following twelve questions will help you quickly determine, during an initial meeting or when reviewing a proposal, whether a supplier is truly suitable for procurement. Two of the questions (eleven and twelve) address aspects that are rarely found in standard checklists but have proven highly relevant in practice.

Each question follows the same structure: a key statement, a checklist, context, a substantive answer pattern, a warning sign, and a brief statement about new direction's own position. You can use the guide as is, adapt it to internal audit processes, or use it as the basis for a written supplier survey.

01 Certifications in everyday life

CHECKS WHETHER CERTIFICATES ARE ACTUALLY USED IN EVERYDAY DEVELOPMENT WORK.

What certifications do you hold, when was the last audit, and how are the associated processes applied in your daily development work? ISO 9001 certification is rarely sufficient in safety-critical environments. What matters is proof that processes are standardized and audited, and that developers can explain the requirements themselves.

> A SUBSTANTIAL ANSWER
>
> Current TISAX audit with high protection requirements, EcoVadis Gold or comparable rating, concrete audit data with expiry horizon, visible implementation in CI/CD pipelines and release paths.

> WARNING SIGNS
>
> Certificates appear permanently "in planning", audit data is missing, and developers do not know the underlying requirements.

NEW DIRECTION ADDS: TISAX audit passed in 2025, valid until 2028. EcoVadis Gold certification currently in place. ISO 27001 certification is in preparation. All developers undergo an eight-hour security and process onboarding course.

02 Security status of site and personnel

EXAMINES: THE SPATIAL AND PERSONNEL ACCESS BARRIER TO CLASSIFIED INFORMATION.

Is your location security-cleared, and how many employees have currently undergone security clearance? For contracts in defense, government, and dual-use contexts, physical and personnel access barriers are a prerequisite, not an add-on.

> A SUBSTANTIAL ANSWER
>
> Security-vetted location in the country, personnel with defined vetting status, onshore development, clear statement on the number of vetted persons with date.

> WARNING SIGNS
>
> Evasive answers regarding subcontractors, fragmented development in unclear legal jurisdictions, figures without a time reference.

NEW DIRECTION ADDS: Security-cleared location in Augsburg. A proportion of security-cleared personnel are employed within the framework of ongoing mandates; expansion is in preparation. Purely onshore development without offshore components.

03 Standards and norms of one's own domain

CHECKS: WHETHER THE PROVIDER CAN HONESTLY STATE THEIR OWN STATUS PER STANDARD.

Which domain-specific standards do you work with (e.g., DO-178C, EMAR, STANAG 4586, ISO 26262, Automotive SPICE), and how transparently do you describe your status for each standard? Approval and procurement capability depend less on a supplier's knowledge of standards than on their ability to actually provide the necessary evidence (traceability, test coverage, documentation).

> A SUBSTANTIAL ANSWER
>
> Clear distinction between "certified", "experienced in", "oriented towards" and "in preparation". References to specific predecessor projects in which the evidence was provided.

> WARNING SIGNS
>
> Standards are listed in general terms, without the provider being able to specify their own status for each standard.

NEW DIRECTION IN THIS REGARD: Our standards map (module 06 of this library) specifies the actual status of each standard. TISAX certified. Experienced in ISO 26262 and Automotive SPICE. Based on DO-178C, EMAR, and STANAG 4586.

04 References with comparable criticality

CHECKS: THE TRANSFERABILITY OF EXISTING EXPERIENCE TO THE PLANNED TASK.

What references from comparable levels of criticality and regulation can you provide, and which of these may be openly communicated? A supplier with exclusively civilian references may be technically capable, but lacks experience in administrative processes and procurement logic.

> A SUBSTANTIAL ANSWER
>
> Specific mention of clients and contract types, clear separation between projects that can be shown openly and those that can be mentioned under confidentiality, transferability to your order can be specified.

> WARNING SIGNS
>
> References remain vague, names are routinely redacted, and levels of criticality are not discussed.

NEW DIRECTION ALSO: Public: BMW EMV for over 20 years, TÜV Süd, GFAW STAR system takeover, BM-DS Ground Control Station Ghost 150. Anonymized: .NET specialist applications of a national defense 2024 to 2028.

05 Contract models and lifecycle perspective

CHECK WHETHER THE PROVIDER THINKS IN TERMS OF PROJECT DURATIONS OR LIFECYCLES.

What contract models do you offer for maintenance, support, and change requests, and how long do you typically support systems? Software contracts in the government and defense sector often run for four to eight years and require a partner who can deliver reliably over this period.

> A SUBSTANTIAL ANSWER
>
> Verifiable customer relationships spanning ten or twenty years, standardized maintenance contracts, change request processes with documented lead times, and obsolescence management as an explicit component.

> WARNING SIGNS
>
> The provider thinks in terms of projects, not lifecycles. Support ends after project acceptance. Change requests are negotiated on an ad hoc basis.

NEW DIRECTION ADDS: Longest ongoing customer relationship: 25 years. Maintenance and change request processes documented. Current contracts in the defense technology sector with a four-year term.

06 Responsiveness and service quality

CHECKS WHETHER REACTION TIMES ARE DEFINED IN A BINDING MANNER OR ARE PURELY ASPIRATIONAL.

Within what timeframes do you respond to initial inquiries, what is your response guarantee in the event of disruptions, and through which channels do you communicate? Public sector procurement operates with clearly defined response times. A supplier who cannot transparently state these times quickly becomes a bottleneck in ongoing processes.

> A SUBSTANTIAL ANSWER
>
> Promised initial response within a few working days under NDA, defined service hours with personal availability, dedicated email mailboxes for procurement officers, encrypted communication on request.

> WARNING SIGNS
>
> Response times are not guaranteed. Inquiries are handled via general sales email addresses. Encrypted communication is a marketing claim without technical basis.

NEW DIRECTION ADDS: Guaranteed initial response to procurement inquiries within five business days under NDA. Dedicated mailbox: getintouchwith@newdirection.de. PGP available upon request. Service hours: Monday to Friday, 8:00 AM to 5:00 PM.

07 Language skills and experience with public authorities

TESTS: OPERATIONAL LANGUAGE SKILLS IN AN ADMINISTRATIVE AND PROCUREMENT CONTEXT.

What languages does your operational team cover, and what procurement processes are you proficient in? Friction caused by language barriers or a lack of knowledge of procurement law significantly slows down procurement processes and is examined during the award procedure.

> A SUBSTANTIAL ANSWER
>
> Native speaker coverage in German and English, also French and Italian for Switzerland, direct experience with WTO procurement, self-declaration BKB, Swiss Procurement Conference.

> WARNING SIGNS
>
> Communication is only possible via intermediaries or external translators. Initial experience with public procurement law is still pending.

NEW DIRECTION ALSO INCLUDES: German, English, and French operationally covered. Permanent representation of Switzerland in St. Gallen. WTO-related tendering procedures last successfully completed in 2023.

08 Export control and compliance

CHECKS WHETHER THE PROVIDER CONDUCTS DUAL-USE TESTING AS AN OPERATIONAL PROCESS.

How do you assess your services for export control relevance, and how is the internal process organized for dual-use classification? Software components in the defense and high-tech sectors may fall under Regulation (EU) 2021/821 and the Foreign Trade and Payments Act.

> A SUBSTANTIAL ANSWER
>
> Established internal review process with documented responsibility, clear handling of third-party libraries, description of the decision logic for order review.

> WARNING SIGNS
>
> Ignorance of dual-use regulations. Reliance on external advice without internal accountability.

NEW DIRECTION ADDS: Internal compliance responsibility has been appointed. Every request undergoes an export control check. Contact person: compliance@newdirection.de.

09 Transfer of existing systems

TESTS: THE ABILITY TO SEAMLESSLY CONTINUE FOREIGN CODEBASES.

Do you have experience in taking over an existing system from a previous service provider without interrupting operations? Rarely does a project start from scratch. Often, it involves continuing a system that is handed over with limited documentation or personnel.

> A SUBSTANTIAL ANSWER
>
> Standardized takeover process, documented references for seamless transitions, code audit and refactoring strategy without operational disruption.

> WARNING SIGNS
>
> The provider is demanding a complete rebuild because they are refusing to integrate foreign code.

NEW DIRECTION ADDS: Two system takeovers successfully completed in 2023 and 2024, one of them in the public sector. Standardized takeover process documented in four phases (module 05 of this library).

10

Ownership structure and sovereignty

CHECKS: THE OWNERSHIP CONTROL OVER SOURCE CODE AND DATA.

How is your company's ownership structure organized, and what control over source code and data do you actually have? In the defense and regulatory context, clients are increasingly scrutinizing the ownership sovereignty of their suppliers.

> A SUBSTANTIAL ANSWER
>
> Clear information on the ownership structure, no opaque shareholdings, source code and data storage in the country, no dependence on suppliers outside the agreed legal area.

> WARNING SIGNS
>
> The ownership structure is answered evasively when asked. Source code and data are located in changing cloud regions.

NEW DIRECTION ADDS: 100 percent German owners. No foreign investments. Source code repositories located in Germany. Data stored in certified German data centers.

11 Insolvency prevention and business continuity assurance

CHECKS: WHAT HAPPENS TO YOUR SYSTEM IF YOUR SUPPLIER BECOMES INSOLVENT.

Procurement processes rarely consider the supplier's financial stability over the contract term. For safety-critical systems with long-term commitments, an unannounced insolvency can lead to system shutdown. A professional supplier will have made provisions for this eventuality and will disclose these provisions transparently.

> A SUBSTANTIAL ANSWER
>
> Source code escrow with a notarial deposit service, contractual agreement for the transfer of rights to the client in the event of insolvency, documented handover procedures, safeguarding of operational capability for at least 90 days after filing for insolvency.

> WARNING SIGNS
>
> The issue is dismissed as unlikely; there is no escrow arrangement, no documented procedure for insolvency, and no robust capital structure.

NEW DIRECTION ADDS: Escrow agreements with notarial escrow services are being prepared for all long-term mandates. Documented handover procedure. Solid equity base. In operation since 1998.

12

Temporary staff access to source code and data

EXAMINES: THE GREY AREA OF ACCESS CONTROL FOR WORKING STUDENTS, INTERNS, AND EXTERNAL CONSULTANTS.

How do you regulate access to source code and test data for student employees, interns, and external consultants in your projects? Most certifications regulate permanent staff. Temporary workers and external consultants often operate in a gray area. In safety-critical projects, this gray area is precisely the most frequent point of entry for compromise.

> A SUBSTANTIAL ANSWER
>
> Clear regulations for security checks of temporary staff, documented access rights per role, technical separation of sensitive areas, automated deletion of access after contract termination, onboarding and offboarding procedures.

> WARNING SIGNS
>
> Student employees have blanket repository access, external consultants work remotely without controlled access, and there are no documented procedures for terminating access.

NEW DIRECTION ADDS: Working students and interns work exclusively on unclassified projects. Role-based access rights. Automated offboarding procedure with access revocation on the day of departure.

FOR FURTHER EXCHANGE

This guide is part of our procurement library.

Five additional documents are available for free download in the same library. For questions regarding specific checklist points or the application of the guide to concrete procurement procedures, please contact us at getintouchwith@newdirection.de within five business days. Confidentiality is guaranteed upon request.

EMAIL FOR PROCUREMENT OFFICERS

getintouchwith@newdirection.de

SWISS REPRESENTATION

St. Gallen · +41 71 45522-57