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

CONFIDENTIALITY AGREEMENT

Bilateral confidentiality agreement.

Template for initial discussions and technical explorations between new direction and procurement departments, system manufacturers, or consortium partners. Bilingual German and English. The German version prevails in case of interpretation.

TEMPLATE	APPLICATION	BUILDING BLOCK	SENDER
Bilingual DE/EN	Initial consultations	2 of 6	new direction GmbH

BETWEEN	AND
	new direction GmbH
Address	Main Street 7, 86356 Neusäß
Represented by	Represented by the management
— HEREINAFTER REFERRED TO AS "PARTY A" —	— HEREINAFTER REFERRED TO AS "PARTY B" —

The parties intend to exchange confidential information during an initial consultation or technical assessment. For this purpose, they agree to the following provisions. This template is a sample document and does not replace individual legal review. It may be replaced by a document provided by the disclosing party.

The parties intend to exchange information of a confidential nature within the scope of an initial meeting or technical exploration. To this end, they agree on the commission set out below. This

template constitutes a draft and does not replace legal review in individual cases. It may be superseded by the disclosing Party's own template.

§ 1 Purpose

Purpose

The purpose of this agreement is to explore potential cooperation in the field `Project title` The information disclosed during this audit will be handled in accordance with this agreement.

The purpose of this Agreement is the evaluation of a potential cooperation in the field of `[Project Name]` . Information disclosed in the course of this evaluation shall be handled in accordance with this Agreement.

§ 2 Confidential information

Confidential Information

Confidential information includes all technical, economic, legal, and other details, documents, source codes, specifications, knowledge, and insights that one party discloses to the other within the scope of the purpose in written, electronic, oral, or tangible form and that are recognizable as confidential by their content or marking.

Confidential Information means all technical, commercial, legal and other data, documents, source code, specifications, know-how and findings disclosed by one Party to the other in the course of the Purpose in written, electronic, oral or embodied form and which are recognizable as confidential by content or marking.

§ 3 Obligations of the receiving party

Obligations of the Receiving Party

The receiving party undertakes to

1. Confidential information shall be used exclusively for the purpose agreed upon in Section 1.
2. to protect them with the same care with which it protects its own confidential information, but at least with the care of a prudent businessperson,
3. to make them accessible only to those employees, agents or consultants who need to know them for this purpose and are subject to an equivalent duty of confidentiality.

The receiving party undertakes to

1. use Confidential Information solely for the Purpose defined in Section 1,
2. protect it with the same care as it protects its own confidential information, in any event with the care of a diligent business,
3. disclose it only to employees, agents or advisors who need to know it for the Purpose and who are bound by equivalent confidentiality obligations.

The obligation of confidentiality does not apply to information that

1. were already publicly known at the time of disclosure or become publicly known through no fault of the receiving party,
2. which were demonstrably already known to the receiving party prior to disclosure,
3. demonstrably developed independently by the receiving party without the use of Confidential Information,
4. must be disclosed due to legal regulations, official orders or legally binding decisions, with the receiving party informing the disclosing party without delay.

The confidentiality obligation shall not apply to information that

1. was already publicly known at the time of disclosure or becomes publicly known without fault of the receiving Party,
2. was demonstrably known to the receiving party prior to disclosure,
3. was demonstrably developed independently by the receiving Party without use of the Confidential Information,
4. must be disclosed by statutory provision, administrative order or final court decision, in which case the receiving Party shall promptly inform the disclosing Party.

§ 5

Disclosure to third parties

Disclosure to Third Parties

Disclosure of Confidential Information to third parties, including affiliated companies and subcontractors, requires the prior written consent of the disclosing party. The receiving party shall ensure that any authorized third parties are subject to an equivalent confidentiality obligation.

Disclosure of Confidential Information to third parties, including affiliates and subcontractors, requires the prior written consent of the disclosing Party. The receiving party ensures that approved third parties are bound by equivalent confidentiality obligations.

§ 6

No transfer of rights

No Transfer of Rights

This agreement does not establish any transfer of ownership, copyright, patent, trademark, or other intellectual property rights. Confidential information remains the property of the disclosing party.

This Agreement shall not effect any transfer of ownership, copyright, patent, trademark or other intellectual property rights. Confidential Information shall remain the property of the disclosing Party.

§ 7

Duration and return

Term and Return

This agreement enters into force upon signature by both parties. The confidentiality obligation lasts for the duration of `three years` This applies after the conclusion of the exploratory phase or termination of the cooperation. Upon written request from the disclosing party, confidential information, as well as all copies and extracts, must be returned immediately or verifiably destroyed. Destruction must be confirmed in writing upon request.

This Agreement enters into force upon mutual signature. The confidentiality obligation shall remain in effect for a period of `three years` after conclusion of the exploration or termination of the cooperation. Upon written request of the disclosing Party, Confidential Information and all copies and excerpts shall be promptly returned or verifiably destroyed. Destruction shall be confirmed in writing upon request.

The breaching party shall be liable for damages arising from a breach of this agreement in accordance with statutory provisions. Further rights, in particular claims for injunctive relief, remain unaffected. The parties acknowledge that a breach of confidential information may result in substantial damages that cannot be fully compensated by monetary damages.

The breaching Party shall be liable for damages resulting from a breach of this Agreement in accordance with statutory provisions. Further rights, in particular claims for injunctive relief, shall remain unaffected. The Parties acknowledge that a breach of Confidential Information may lead to substantial damages that cannot be fully compensated by monetary damages.

§ 9 Applicable law and jurisdiction

Governing Law and Jurisdiction

This agreement is subject to the law of Federal Republic of Germany excluding the UN Convention on Contracts for the International Sale of Goods (CISG). The exclusive place of jurisdiction for all disputes arising from or in connection with this agreement is [location]. augsburg .

This Agreement shall be governed by the laws of the Federal Republic of Germany , excluding the UN Convention on Contracts for the International Sale of Goods. The exclusive place of jurisdiction for all disputes arising out of or in connection with this Agreement shall be Augsburg .

§ 10 Final Provisions

Miscellaneous

Amendments and additions to this agreement must be in writing. This also applies to any waiver of this written form requirement. Should any provision of this agreement be or become invalid, this shall not affect the validity of the remaining provisions. The invalid provision shall be replaced by a provision that most closely approximates its intended economic purpose.

Amendments and additions to this Agreement require written form. This also applies to the waiver of the written form requirement. Should any provision of this Agreement be or become invalid, this shall not affect the validity of the remaining provisions. The invalid provision shall be replaced by a provision that comes closest to the intended commercial purpose.

SIGNATURES

PARTY A	PARTY B · NEW DIRECTION GMBH
PLACE, DATE	PLACE, DATE
SIGNATURE	SIGNATURE
NAME, FUNCTION · NAME, TITLE	NAME, FUNCTION · NAME, TITLE

NOTICE

This template is a sample draft. It does not replace legal review in individual cases. For engagements with classified content or security clearance relevance, additional agreements may be required. New direction GmbH alternatively accepts the disclosing party's own non-disclosure template.

SUPPLIER SELF-DISCLOSURE

Structured template for the initial screening of software suppliers.

This template compiles the information that procurement officers typically request. The middle column shows an example of the information provided by New Direction. The right-hand column remains empty for the supplier being evaluated.

TEMPLATE	SCOPE	BUILDING BLOCK	STATUS
German	8 areas	3 of 6	1/2026

AREA 01 · BASIC DATA

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Company name, legal form	*new direction GmbH*	
Registered office and commercial register	*Neusäß, HRB Augsburg*	
Year of foundation	*1998*	
Other locations	*Branch office St. Gallen, Switzerland*	

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
VAT ID	*DE...*	

AREA 02 · OWNERSHIP AND STRUCTURE

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Ownership structure	*100% German owners, no foreign investment*	
Group affiliation	*No, independently*	
Management	*Michael Robert Biber, Stephan Weber*	
Investments in third parties	*No*	

DEPARTMENT 03 · PERSONNEL

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Number of employees (as of the reference date)	*Approximately 30, including the engineering team at the Neusäß site*	
Percentage of permanent employees	*Over 90 percent*	
Security-vetted personnel	*Within the scope of ongoing mandates, expansion is in preparation.*	
operational language competence	*German, English, French*	
Longest period of service	*Over 24 years*	

SECTION 04 · REFERENCES

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Current Aerospace Mandate	*Ground Control Station Ghost 150, BM-DS AG*	
Current Defense Mandate	*.NET specialist applications for national defense, 2024 to 2028*	
Current public sector mandate	*Further development of the STAR system, GFAW Thuringia*	
Longest industrial relationship	*BMW Group, over 20 years (EMC measurement data)*	
Further references	*TÜV Süd, Audi, SIXT, Europcar, AL-KO, APZ, RENK*	

SECTION 05 · CERTIFICATIONS AND STANDARDS

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
TISAX	*Certified, expiry 2028*	
EcoVadis	*Gold, currently*	
ISO 27001	*In preparation*	

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Domain standards	*See module 06 Standards map*	
Research Seal of the Donors' Association	*"Innovative through research"*	

AREA 06 · COMPLIANCE AND TAXES

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Tax and social security status	*No residues, certificate of conformity available upon request*	
Export control process	*Internal audit process established in accordance with EU 2021/821 and AWG*	
Self-declaration BKB	*Fulfilled*	
Self-declaration Switzerland	*Compliant with Swiss Procurement Conference standards*	
Compliance contact person	*compliance@newdirection.de*	

AREA 07 · EXISTENCE AND CONTINUITY

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Source code escrow	*In preparation for all long-term mandates*	
Business Continuity	*Documented handover procedure, operational capability 90 days after insolvency*	
auditors	*Upon request*	
Professional liability insurance	*Existing, coverage details available upon request*	

DEPARTMENT 08 · CONTACT FOR PROCUREMENT

INFORMATION	NEW DIRECTION (EXAMPLE)	YOUR COMPANY
Procurement mailbox	*getintouchwith@newdirection.de*	
First Response SLA	*Five working days under NDA*	
Service hours	*Mon to Fri 8am to 5pm*	
Encrypted communication	*PGP available upon request*	

SECURITY QUESTIONNAIRE

Answer templates for security questionnaires from prime agents and procurement officers.

The template follows the structure of ISO 27001 Annex A. It comprises ten core areas and provides reference answers that serve as a starting point for completing individual questionnaires. The answers are factual and do not include any project-specific information.

STRUCTURE	SCOPE	BUILDING BLOCK	STATUS
ISO 27001 Annex A	10 areas	4 of 6	1/2026

Clients in the defense and government sectors typically send out multi-page security questionnaires before initiating deeper collaboration. These questionnaires vary in length and level of detail, but generally follow a recurring structure.

The following ten areas correspond to the core domains of ISO 27001 Annex A and cover the audit topics that appear in most questionnaires. For each area, we formulate a reference answer, as new direction provides it in an initial consultation.

A.5

Information security guidelines

Does your company have a documented information security policy? Who is responsible for it? When was it last revised?

REFERENCE RESPONSE

Yes. Approved and regularly reviewed by management, last revised as part of the TISAX audit in 2025. Core policy supplemented by specific procedural instructions for development, access and incident management.

A.6

Information security organization

Who bears operational responsibility for information security? How are roles and the separation of tasks regulated?

REFERENCE RESPONSE

Designated Information Security Officer with a direct reporting line to management. Separation of operational and auditing roles. External audit support by a TISAX-accredited auditing service provider.

A.7

Personal safety

How are employees and external staff vetted before starting work? How are onboarding and offboarding handled with regard to access and obligations?

REFERENCE RESPONSE

Background checks and police clearance certificates for security-relevant roles. Security clearances for personnel in classified mandates. Eight-hour security onboarding for all new employees. Automated offboarding procedure with access revocation on the day of departure.

A.8

Asset Management

How are information values identified, classified, and assigned to the responsible party? How are classification levels implemented technically?

REFERENCE RESPONSE

Central asset catalog with classification according to confidentiality, integrity, and availability. Classification follows client requirements. Implementation in access rights, encryption, and backup protocols.

A.9

Access control

How is access to systems and information granted and regularly reviewed? How are privileged accesses controlled?

REFERENCE RESPONSE

Role-based access control. Multi-factor authentication for all critical systems. Quarterly recertification of permissions. Privileged access is time-limited and logged.

A.10

Cryptography

Which cryptographic methods are used? How is key management handled?

REFERENCE RESPONSE

Exclusively procedures according to BSI TR-02102 and current recommendations. Symmetric AES-256, asymmetric RSA-4096 or elliptic curves. Central key management with documented lifecycle.

A.11

Physical security

How is the physical security of the business premises organized? Access controls, video surveillance, visitor regulations?

REFERENCE RESPONSE

Security-approved location in Augsburg with access control, documented visitor policy, and video surveillance of public areas. Server rooms are separately secured. Cleaning staff are bound by confidentiality agreements.

A.12

Operational safety

How are patch management, malware protection, and backups handled? What logs are kept and for how long?

REFERENCE RESPONSE

Automated patch management, critical security patches within defined timeframes. Endpoint protection on all systems. Backup concept based on the 3-2-1 rule with offline copy. Log retention for at least one year, longer for security-relevant events.

A.14

Application safety

How is security integrated into the development process? Code reviews, static analysis, test coverage, release processes?

REFERENCE RESPONSE

Security by Design as a process requirement. Four-eyes principle for code reviews. Static analysis in the CI pipeline. Dependency scanning for open-source components. Test coverage based on criticality, documented release paths.

A.16

Incident Management

How are security incidents detected, reported, and handled? What reporting deadlines apply to clients?

REFERENCE RESPONSE

Documented incident response process. Notification to the client within the contractually agreed timeframes, generally within 24 hours for security-related incidents. Post-incident reviews with the derivation of corrective actions.

A.17

Business Continuity

What measures are in place to ensure continued operational capacity? Recovery targets, redundancies, insolvency provisions?

REFERENCE RESPONSE

Documented business continuity concept. Redundant development environments. Recovery goals defined per order. Source code escrow in preparation. Operational capability documented 90 days after insolvency filing.

A.18

Compliance

Which legal and contractual requirements are systematically monitored? How is this verified?

REFERENCE RESPONSE

Compliance register with all relevant regulations (GDPR, EU 2021/821, AWG, TISAX requirements, industry-specific standards). Regular internal audits. External audits by TISAX and EcoVadis. Compliance contact: compliance@newdirection.de.

USING THIS TEMPLATE

This answer template is a starting point, not a finished questionnaire.

Each client uses their own questionnaire with specific wording and additional questions. The reference responses in this template serve as a baseline that must be adapted to the specific questions at hand. For project-specific adjustments, especially for classified mandates, please contact us at getintouchwith@newdirection.de.

COMPLIANCE CONTACT PERSON
compliance@newdirection.de

PROCUREMENT MAILBOX
getintouchwith@newdirection.de

Four phases for taking over a system from a previous service provider.

Practical guide for seamless handovers without business interruption. Developed from two system takeovers in 2023 and 2024, one of which was in the public sector.

STRUCTURE	SCOPE	BUILDING BLOCK	STATUS
Four phases	Approximately 30 checkpoints	5 of 6	1/2026

Taking over an existing system from a previous service provider is one of the most challenging moments in a long-term software project. The stakes are high because a mistake during the handover can have repercussions for years. Visibility is low because external observers don't see the actual work involved.

This checklist divides the takeover process into four phases with clear checkpoints. Essentially, it serves as a user manual for procurement managers overseeing a supplier change. It can be used simultaneously by both the outgoing and incoming suppliers.

01 Prior to the acquisition (due diligence)

TIMEFRAME: 4 TO 6 WEEKS BEFORE HANDOVER

- [ ] Check the completeness of the handover documentation (architecture, operating manual, data model, interfaces)

  Missing documentation is the most frequent issue. Early inclusion in the handover protocol creates binding obligations.

- [ ] Identify repository status and access methods (Git history, branches, tags, completeness)

  An incomplete repository that is only delivered and not historically preserved blocks long-term maintenance.

- [ ] Review ticket history and submit change request backlog

  Open tickets from the predecessor's era reveal the true system weaknesses.

- [ ] Identify contractual relationships with suppliers and third-party components

  Forgotten supplier contracts are a typical cost trap in the first year of operation.

- [ ] Check licenses and usage rights (open source, commercial, contract rights)

  Libraries used by the predecessor under proprietary licenses must be handed over in a documented manner.

- [ ] Inventory technical debt and prioritize it with the client.

  Honestly recording technical debt prevents surprises in the third year of operation.

02 Handover period

TIMEFRAME: 4 TO 8 WEEKS IN PARALLEL

- [ ] Define parallel operation (responsibilities, reporting channels, release paths)
  Who decides on change requests during the transition phase? Document a clear, written agreement.
- [ ] Conduct knowledge transfer sessions with key personnel from the predecessor.
  Recording sessions with mutual consent reduces later follow-up questions.
- [ ] Establish communication channels and name contact persons
  The client must know at all times whom he is addressing.
- [ ] Set up test environments and compare them with the production environment.
  Discrepancies between testing and production are standard errors during system takeovers.
- [ ] Implement your first own change requests to understand the system from a user's perspective.
  A simulated small change request during the handover phase reveals process gaps.

03 takeover

TIMEFRAME: DEADLINE FOR ASSUMING RESPONSIBILITY

- [ ] All access data is being rotated (databases, systems, external services).
  The predecessor must no longer have operational access after the cut-off date.
- [ ] Take over deployment pipelines and migrate them to your own infrastructure
  The predecessor's pipelines are often tied to its CI/CD landscape. Early migration reduces the risk of failure.
- [ ] Test and document backup and restore procedures
  A restore test in the first week after the takeover immediately shows whether the transferred backups are usable.
- [ ] Switch monitoring and alerting to your own systems
  Blackouts often occur because alerts are still being routed to the predecessor.
- [ ] Update operating manuals and final release of communication channels
  The client and other parties involved must receive the new contact details in writing.

04 After the takeover

TIMEFRAME: FIRST 30, 90 AND 180 DAYS

- [ ] First 30 days: close monitoring, daily status check
  System stability is not yet guaranteed. Errors from the handover phase are now coming to light.
- [ ] First 90 days: implement your first own change requests and validate response times
  During this phase, the client checks whether the promised service times are realistic.
- [ ] First 180 days: Retrospective together with the client
  A documented retrospective after six months is the best anchor of trust for the coming contract years.
- [ ] Resolve remaining open issues from the takeover
  Issues that were postponed to "later" during the handover phase risk remaining permanently unresolved.

SUPPLEMENT TO THIS CHECKLIST

The checklist is based on two system takeovers.

In 2023, we successfully completed the takeover of the STAR system from a predecessor service provider on behalf of GFAW Thüringen without any operational interruption. In 2024, we acquired .NET applications for a national defense agency as part of a WTO-approved tender process. Both takeovers resulted in the audit points listed here. Please contact us if you have any questions regarding the application of this checklist.

PROCUREMENT MAILBOX
getintouchwith@newdirection.de

SWISS REPRESENTATION
St. Gallen · +41 71 45522-57

STANDARDS MAP

Honest status information per standard.

Overview of the standards that New Direction is working on, with a clear indication of their current status. This map forms the basis for the statements in the Procurement Guide, the Self-Assessment, and the Security Questionnaire.

SCOPE	UPDATE	BUILDING BLOCK	STATUS
8 Standards	Quarterly	6 of 6	1/2026

Suppliers in the defense and regulatory sectors tend to list all the standards they have encountered as equally valid. This creates confusion. A procurement officer can no longer determine which standards to rely on based on such a list.

We differentiate between five status levels for each standard. This differentiation is intentionally restrictive. Inclusion in the "Certified" category is only granted upon presentation of a current certificate. Inclusion in the "Experienced in" category is only granted if we can demonstrate concrete projects.

STANDARD	DOMAIN	STATUS AT NEW DIRECTION
TISAX	Information security in the automotive environment	Certified
EU 2021/821	Dual-Use Regulation	Complied with
ISO 26262	Functional Safety Automotive	Experienced in
Automotive SPICE	Software Maturity Level Automotive	Experienced in
DO-178C	Software in civil aviation	Based on
EMAR	Military airworthiness	Based on
STANAG 4586	UAV interoperability	Based on
ISO 27001	Information Security Management System	In preparation

`Certified.` A current certificate from an accredited testing laboratory is available. We will provide the issue and expiry dates upon request.

`Compliant.` Legal requirements are continuously met within the framework of established internal processes.

`Experienced in.` We have provided the relevant evidence (traceability, test coverage, documentation) in specific projects.

`Oriented towards.` We align our work with the methodology of the standard, but are not certified and do not provide formal proof of conformity.

`In preparation.` An audit process has been initiated or process preparation is underway. We will provide specific information on the status upon request.

UPDATE NOTICE

This map is updated quarterly. We actively communicate any status changes to clients with ongoing contracts. For procurement officers in active bidding processes, we provide written confirmations regarding the status of selected standards upon request.