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