CADIS - Cybersecurity Assessment for Defence Industry Suppliers

Whitepaper CADIS

The defence industry is more dependent than ever on robust, secure, and resilient supply chains. Geopolitical tensions and new regulatory requirements, such as the NIS2 directive, the German Federal Office for Information Security Act (BSIG), and the Cyber Resilience Act, as well as the increasing digitalization of value chains, present a shared challenge to manufacturers and suppliers: demonstrating cybersecurity at every level of the supply chain.

Background

Existing standards such as ISO/IEC 27001 and TISAX address important aspects of cybersecurity, but they do not comprehensively cover the specific requirements of the defence and armaments industry. CADIS goes beyond these standards by introducing a dedicated Operational Technology (OT) module for securing production and control systems in accordance with IEC 62443, tiered special requirements for suppliers, with elevated criticality, geopolitical risks, and geographic location as mandatory criteria in supplier evaluations, a dedicated module for the responsible use of Artificial Intelligence based on ISO/IEC 42001, and a separate module for the transportation and handling of security-relevant goods. This creates an assessment framework that reflects the realities of security-critical supply chains, rather than forcing them into an industry-neutral standard.
As the first European assessment scheme specifically designed for suppliers to the defence industry, CADIS establishes a consistent, transparent, and measurable foundation for cybersecurity throughout the supply chain and closes this gap. Developed and conducted exclusively by DEKRA, the scheme combines 14 modular assessment areas, ranging from physical security and IT and OT security to data protection, compliance, and AI governance, and aligns them with the requirements of ISO/IEC 27001:2022, IEC 62443, NIST CSF v2.0, BSI IT-Grundschutz, NIS2, BSIG, GDPR, and the Cyber Resilience Act.

Your Benefits

- **Market Access:** Be recognized as a reliable partner in the defence and armaments industry and qualify for security-relevant contracts.
- **Competitive Advantage:** Demonstrable cybersecurity builds trust among system manufacturers, government authorities, and insurers, strengthening your market position relative to competitors.
- **Efficiency:** One audit, multiple stakeholders. Through the standardized CADIS Result Exchange, you can securely share your assessment results with requesting customers and avoid duplicate assessments.
- **Regulatory Assurance:** NIS2, BSIG, and the Cyber Resilience Act are systematically addressed, with clear alignment to ISO/IEC 27001, IEC 62443, and NIST CSF.
- **Proportionate Assessment Depth:** Three Levels of Examination (LoE 1–3) and three tiers of Special Requirements tailor the assessment to your risk profile, not the other way around.
- **Measurable Results:** The Security Score (0.00–3.00) is calculated as the weighted sum of all assessment modules and provides a comparable measure of cybersecurity maturity across your organization, over time, and in comparison with customer requirements. Clear thresholds (≥ 2.75 Compliant, 1.01–2.74 Non-Critical Deviation, ≤ 1.00 Critical Deviation) assign the result to one of three assessment outcome categories.

Who Is Affected?

If, as a supplier or service provider, you deliver design data, components, or services to the defence industry, you are increasingly required to demonstrate your cybersecurity capabilities to OEMs, government authorities, and insurers. CADIS is designed for organizations throughout the entire supply chain, regardless of size or field of activity:

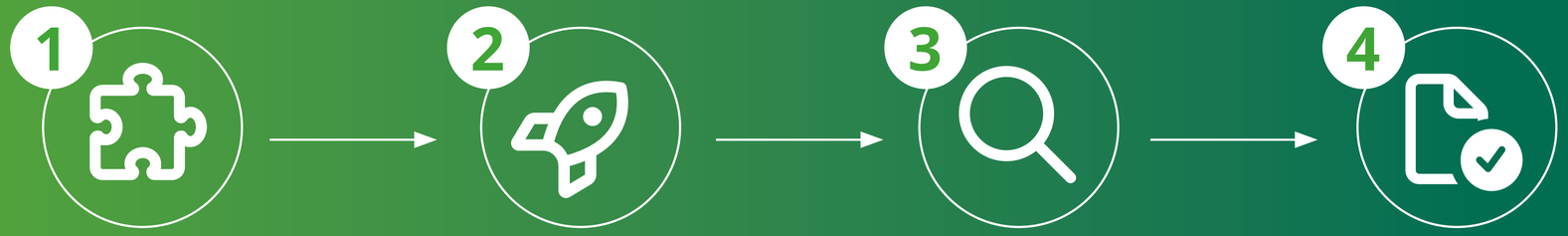
- Direct suppliers to system manufacturers
- Sub-suppliers in multi-tier value chains
- Cloud and managed service providers with access to engineering data
- Service providers handling design and prototype information
- Logistics partners handling classified or security-relevant goods
- Operators of critical OT environments in production and manufacturing

CADIS Is More Than a Checklist

The assessment does not simply evaluate whether a measure exists, but how mature, effective, and demonstrably it has been implemented. Using a rating scale from 0 to 3, DEKRA auditors assess whether measures are documented, implemented, actively practiced, and continuously improved. The principle of proportionality takes into account the organization's size, industry, and risk profile. At the same time, the assessment methodology remains consistent and comparable across all participants.

The CADIS Model: 14 Modular Assessment Areas

1. Physical Site Security
2. Information Security Organization
3. Use of Cloud-Based and External Services
4. Secure Software Development
5. Information Security in Project Management, Human Resources, and Procurement
6. Incident and Crisis Management
7. Business Continuity Management (BCM)
8. Identity and Access Management (IAM)
9. IT Security
10. Operational Technology (OT)
11. Compliance Management
12. Data Protection
13. Use of Artificial Intelligence
14. Transportation and Handling



Participation in Four Steps

Step 1: Assessment Scope (SCE and Scope Definition)
The client defines the assessment scope based on the Supplier Criticality Evaluation (SCE). The SCE considers security relevance, technological dependencies, regulatory requirements, and the supplier's geopolitical risk profile.

Based on the SCE, the applicable level of examination (LoE 1–3) and the corresponding special requirements (Levels 1–3) are determined. The assessment scope includes the relevant sites, assessment modules, and the corresponding assessment depth.

Step 2: Kick-off and Preliminary Review (Phase 1)
After the kick-off meeting, during which the process, scope, and points of contact are aligned, the company submits the completed CADIS Assessment Catalog as part of Phase 1. The review verifies that each assessment question has been assigned a maturity level (0–3), that an implementation description has been provided, and that at least one supporting piece of evidence has been referenced. Companies are granted up to three submission attempts.

Step 3: Main Assessment (Phase 2, LoE 1–3)
After the preliminary assessment is successfully completed, the main assessment begins. DEKRA auditors evaluate the assessment modules on-site and remotely at the Level of Examination (LoE 1–3), as defined by the SCE. The assessment is based on document reviews, interviews with relevant personnel, and sample-based effectiveness testing.

The following selected assessment topics supplement these activities:

Selected Assessment Topics
At the organizational level, the assessment examines the extent to which information security is firmly established and actively practiced. This includes everything from security awareness and access control to structured change and patch management processes.

At the technical level, the effectiveness of security controls, backup and recovery concepts, and incident and crisis management capabilities is evaluated.

Additional assessments are conducted for industrial environments to verify the secure segregation of IT and OT systems, as well as the protection of industrial control systems, in accordance with IEC 62443.

Maturity Levels: The CADIS Assessment Methodology
Maturity Levels instead of Checkboxes: CADIS does not merely verify the existence of a measure, but rather, evaluates its implementation based on its comprehensiveness, effectiveness, and demonstrable quality. Using a scale from 0 to 3, auditors evaluate each assessment criterion based on verifiable evidence and the principle of proportionality. They take into account the organization's size, industry, and risk profile.

The result is a realistic picture of an organization's actual cybersecurity maturity rather than merely confirming compliance.

Step 4: Results, Report, and Approval
In the final step, the assessment results are consolidated into a report, provided to the organization, and, upon approval, made available to authorized customers through the CADIS Result Exchange. The report includes maturity levels for each assessment module, the aggregated Security Score, and one of the following three result categories:

- Compliant (score of 2.75–3.00 with no deviations): Approval is granted for up to two years. A risk-based surveillance assessment is conducted the following year.
- Non-critical deviation (score 1.01–2.74 or at least one non-critical deviation): Temporary approval may be granted, provided that a corrective action plan is in place and conditions are met. Reclassification to Compliant is possible once all deviations have been resolved.
- Critical deviation (score 0.00–1.00 or at least one critical deviation): No approval is granted. Deviations must be resolved within three months, followed by a follow-up assessment.

Your Partner for CADIS

CADIS is a proprietary DEKRA program, developed by DEKRA and conducted exclusively by DEKRA. This means that the methodology, auditor qualifications, and the Result Exchange are managed by a single organization: one of the world's leading testing, inspection, and certification providers, with decades of experience in the independent assessment of safety-critical systems.

As the operator of the CADIS program, DEKRA is responsible for the methodology, qualifies the auditors, and manages the central CADIS Result Exchange database. All auditors hold relevant professional qualifications, including CISA, CISM, and ISO/IEC 27001 Lead Auditor certifications, as well as module-specific credentials for OT (IEC 62443), data protection, and AI (ISO/IEC 42001).

Why DEKRA?

- **Exclusive:** CADIS was developed by DEKRA in collaboration with the defence industry and is conducted exclusively by DEKRA.
- **Independent:** Extensive network of qualified auditors, organizationally separated from consulting services.
- **Industry Expertise:** Decades of experience in cybersecurity, industrial assessments, and safety-critical systems.
- **Holistic Approach:** Information security, data protection, OT, AI, and physical security from a single source.
- **Efficient:** One audit, multiple stakeholders through the standardized CADIS Result Exchange.
- **Predictable:** A two-year assessment cycle with clearly defined transition arrangements and corrective action timelines.

Your Next Step

Schedule a no-obligation initial consultation with our experts. Together, we'll determine the scope of your exam, the appropriate level of examination, and the schedule for your first exam.

Contact us! **Learn more!**

Would you like more information?
Visit our website:

dekra-certification.de/en