# Secure Supply Chains for the Defence Industry

Product Sheet CADIS

**Due to increasing technical complexity, international dependencies, and growing cyber risks, companies in the defence and arms industry are facing new challenges. Not only must supply chains be efficient, they must also be demonstrably secure, resilient, and trustworthy.**

CADIS is the first European assessment framework designed specifically for suppliers in this industry. It provides a standardized, objective, and measurable basis for evaluating cybersecurity and information security across the entire supply chain in a transparent, modular, and risk-based manner.

### Your benefits of CADIS

- **Stronger competitive position** – Demonstrably verified security increases customer trust and strengthens your position in tenders.
- **Easier market access** – Improves your chances of being considered in security-critical procurement processes.
- **Planning reliability** – Clear requirements enable structured preparation and reduce uncertainty.
- **Efficiency through modularity** – Only relevant modules are assessed, helping to keep effort and costs manageable.
- **Holistic security approach** – IT, OT, physical security, and organizational processes are considered together.
- **Reduced supply chain risks** – Early identification of weaknesses helps prevent later disruptions.
- **Enhanced credibility** – Companies can position themselves as responsible partners with a strong security culture.

## Why CADIS?

Cybersecurity and resilience are becoming essential requirements. Organizations in the defence industry have a special responsibility to protect classified information, critical data, and complex technologies against internal and external risks throughout the entire supply chain.

**CADIS was developed specifically for this purpose:**
It provides a clearly structured, standardized assessment framework tailored to the security requirements of this highly sensitive sector.

Its modular structure includes 14 flexible assessment modules that depend on the supplier’s role, sensitivity level, and risk profile.

Companies only need to fulfill the requirements relevant to their position in the supply chain.

Supplier evaluations are carried out by the system manufacturer. DEKRA supports this process by providing the “Supplier Criticality Evaluation” tool, a standardized evaluation framework that ensures consistent, transparent definitions of the assessment scope for each supplier.

The framework is suitable for companies with different levels of maturity because the requirements are clearly defined while still allowing flexibility in technical implementation.

## The Assessment Process: Step by Step

### 1. Kick-Off
The assessment process begins with a joint kickoff meeting. During this meeting, all relevant framework conditions are discussed, expectations are clarified, and the assessment process is coordinated. Required documentation and contact persons are also defined.

### 2. Phase 1 – Remote Pre-Assessment
In this phase, a preliminary assessment is carried out based on the submitted documentation. The objective is to gain an initial understanding of the supplier, identify potential risk areas, and prepare for the main assessment.

### 3. Phase 2 – Main Assessment
The execution of the main assessment is based on the Level of Examination (LoE).

- LoE 1: Plausibility assessment of the overall implementation for each assessment point (not requirement-specific in detail). There is no review of supporting documentation.
- LoE 2: A structured remote interview with a risk-based selection of assessment points. Includes more in-depth verification beyond plausibility checks.
- LoE 3: On-site audit including interviews, inspections, sampling, and site walkthroughs. Evidence-based verification.

### 4. Closing Meeting
After the main assessment, we discuss the results with the customer during a closing meeting. This includes aligning on the action plan, follow-up activities (if required), and scheduling the risk-based surveillance assessment for the following year.

### 5. Action Plan
Based on the identified findings, the customer develops a binding action plan. This plan includes specific corrective measures, responsibilities, and realistic implementation timelines.

### 6. Follow-Up
As part of the follow-up process, the implementation of the agreed-upon measures is reviewed and documented. This ensures that identified weaknesses have been addressed sustainably.

### 7. Risk-Based Surveillance Assessment
This assessment is part of the two-year assessment cycle and takes place in the year following the initial assessment. Planning is based on the preliminary assessment results and a risk-based approach that considers the company’s criticality and risk profile, open findings, deviations from the preliminary assessment, and relevant changes, such as organizational or site-related changes, as well as potential security incidents.

### 8. New Assessment Cycle
Once all steps are complete, the assessment process begins again, adjusted to current conditions and the supplier’s evolving risk profile. This ensures continuous and dynamic supplier monitoring.

## The 14 CADIS Modules

1. Physical Security at the Site
2. Information Security Organization
3. IT Security
4. OT Security
5. Use of Cloud-Based and External Services
6. Business Continuity Management
7. Incident and Crisis Management
8. Identity and Access Management
9. Security in Software Development
10. Information Security in Project Management / Human Resources / Procurement
11. Data Protection
12. Compliance Management System
13. Use of Artificial Intelligence
14. Transport and Handling

## Why DEKRA?

- Exclusive Assessment Framework – CADIS was developed by DEKRA and is administered exclusively by DEKRA.
- Deep industry expertise – We have decades of experience in cybersecurity, industrial inspections, and security-critical sectors.
- Independence and credibility – DEKRA is neutral and internationally recognized, with a strong reputation in supply chain security assessments.

As part of the DEKRA service portfolio, CADIS supplements our certification services by providing a structured assessment framework for the standardized evaluation of cybersecurity and information security within the defence and arms supply chain.

In addition, the DEKRA Group offers the following services:

- Assessments for compliance with internal requirements
- Personnel certifications
- Product testing and certification

**Would you like to learn more about CADIS?**
**Find out more now!**

Contact us

Learn more

Would you like more information?
Visit our website:

**dekra-certification.de/en**