



# General Security Requirements for Dutch Government Contracts

Some key considerations for market parties

Navigating ABDO and ABRO in the Dutch public sector

## **Collaborative strategies for legal and compliance teams facing new security regulations**

The Dutch public and defence sectors are undergoing a transformation in information security requirements. The General Security Requirements for Defence Contracts (ABDO 2019) have long set the standard for safeguarding sensitive information in defence-related projects. Now, with the proposed introduction of the **General Security Requirements for Government Contracts (ABRO)**, these requirements are expanding to cover a much broader range of government contracts and suppliers.

Together, ABDO and ABRO will form a comprehensive compliance framework for organisations working with classified or vital government information. For current contracts, ABDO will continue to apply, whereas the expectation is that ABRO will be phased in for future government contracts. While these frameworks introduce new compliance challenges, they also create opportunities for organisations to distinguish themselves as trusted partners in high-stakes environments.

### **1. About ABDO 2019 and the addition of ABRO**

ABDO 2019 is a comprehensive security framework established by the Dutch Ministry of Defence. It applies to all external parties involved in classified or vital defence projects. Rather than a certification, ABDO is an accreditation process overseen by the Military Intelligence and Security Service (MIVD) and is imposed on parties under contract.

The framework is built on five pillars:

- Governance & organisation
- Personnel
- Physical security
- Cybersecurity
- Cloud security

ABRO will extend these five pillars to a wider group of government contracts and suppliers beyond the defence sector. ABRO is designed to complement and expand upon ABDO, often introducing stricter standards and aligning with frameworks such as ISO 27001 and the Dutch government's Baseline Information security (*Baseline Informatiebeveiliging Overheid*, **BIO**). Both ABDO and ABRO demand advanced technical and organisational measures, including air-gapping, trusted roles, and strict access controls.

## 2. Implications for organisations

The impact of ABDO and ABRO is far-reaching, affecting legal, operational, and strategic dimensions:

- Contractual obligations: Organisations must ensure that confidentiality agreements, ownership structures, and subcontractor management are compliant with security requirements.
- Personnel policies: Screening, assignment of trusted roles, and robust incident reporting become essential.
- Incident management: Effective notification, destruction protocols, and authorisation procedures are required to mitigate risks.
- Governance and risk management: Compliance must be maintained throughout the supply chain, with clear oversight and accountability.

Failure to meet these requirements can result in exclusion from tenders, reputational damage, (contractual) penalties and/or (immediate) termination of the contract. Furthermore, non-compliance that leads to national security information being compromised can also be enforced upon under administrative and criminal law. Conversely, proactive compliance can position organisations as preferred partners for government and defence contracts.

Ensuring ABDO and ABRO compliance can be a lengthy process. As such, ensuring that ABDO and ABRO compliance is taken care of in a timely manner is paramount, given that non-compliance with these standards can lead to exclusion from tenders and contracts.

## 3. When do ABDO and ABRO apply?

ABDO and ABRO are relevant in a variety of scenarios, including:

- Delivery of products or services to the Ministry of Defence or its partners: Compliance is mandatory when handling classified information or vital infrastructure.
- Participation in tenders for defence or broader public sector projects: Meeting security requirements may be a prerequisite for eligibility.
- Collaboration with subcontractors in defence or government supply chains: All parties in the chain must adhere to the relevant standards.
- Operation in strategic sectors such as energy, ICT, or logistics: Even indirect involvement in defence or government projects can trigger applicability.

Organisations should assess their current and future activities to determine where these frameworks may impact their operations and strategic opportunities.

## National Security in Government Procurement

Are there **risks** to national security in a government contract?  
If so, the **ABRO security requirements** will apply to (prospective) contractors.

Examples of threats:



Cyberattacks



Data leaks



Sabotage



Espionage

### The 5 pillars for screening at companies



Governance and Organisation



Physical



Cloud



Personnel



Cyber



#### From early 2026, ABRO will be applied as the standard

Ministries, their services, agencies and the police

#### In preparation

Independent administrative bodies (ZBOs), provinces, municipalities, water authorities and vital sectors

#### 4. Looking Ahead: ABRO

ABRO has now become the definitive benchmark for security in government contracts that impact national security. Since its formal entry came into force on 1 January 2026, ABRO introduces stricter security requirements and broader applicability, affecting a significantly wider group of suppliers and service providers. Organisations active in or supplying to the public sector must ensure compliance with these enhanced standards and prepare for the phased implementation deadlines, which run through 2028 for certain entities.

Loyens & Loeff continues to closely monitor these developments and proactively advises clients on the implications of ABRO, enabling organisations to anticipate new compliance obligations and make informed strategic decisions.

## How Loyens & Loeff can help

Loyens & Loeff combines in-depth legal and tax expertise with sector-specific knowledge in defence, the public sector and regulated industries. Our services include:

- Interpreting and applying ABDO/ABRO requirements
- Drafting and reviewing contracts and compliance documentation
- Guiding organisations through the accreditation process
- Structuring governance and risk management
- Training and awareness for internal stakeholders

Would you like to discover how these regulations may impact your organisation? Our experts are ready to help you assess your compliance position, connect with key market players and turn regulatory challenges into strategic opportunities. Contact us for tailored advice or to discuss the latest developments in ABDO and ABRO.

## Our team

### Jan-Willem van Rooij

Attorney at Law, Partner

T +31 10 224 65 52

M +31 6 53 26 01 31

E [jan.willem.van.rooij@loyensloeff.com](mailto:jan.willem.van.rooij@loyensloeff.com)



### Anida Zuko

Attorney at Law, Senior Associate

T +31 10 224 65 69

M +31 6 57 36 81 45

E [anida.zuko@loyensloeff.com](mailto:anida.zuko@loyensloeff.com)



### Nanne Kusters

Attorney at Law, Senior Associate

T +31 20 578 59 11

M +31 6 57 63 88 34

E [nanne.kusters@loyensloeff.com](mailto:nanne.kusters@loyensloeff.com)



#### Disclaimer

Although this publication has been compiled with great care, Loyens & Loeff N.V. and all other entities, partnerships, persons and practices trading under the name 'Loyens & Loeff', cannot accept any liability for the consequences of making use of the information contained herein. The information provided is intended as general information and cannot be regarded as advice. Please contact us if you wish to receive advice on this specific topic that is tailored to your situation.