

Dual-use goods: a new guide for Internal Compliance Program

For the last twenty years, the European and national authorities have forced companies to take responsibility for themselves by enacting the rules they undertake to respect and the violation of which entails sanctions. This has led to the rapid emergence of compliance. As a recent example, the RGPD and the anti-bribery French Law, so-called “Sapin 2”, require companies to implement compliance programs on data protection, for one, and the fight against corruption, for the other. This trend also covers export control, more particularly, dual-use goods.

What are dual-use goods?

It refers to goods, equipment or services (including technology, software or know-how) that can be used for both civilian and military purposes, as well as those that may contribute to the proliferation of nuclear, chemical or biological weapons. **Originally planned for civilian use, they are potentially dangerous if this use is diverted for military or repressive purposes.**

The most classic examples are the use of thermal vision to control the insulation of buildings, but also to identify concealed live targets, or the cryptology that protects computer networks, but may also hide electronic communications between terrorists. Therefore, the European Union Regulation No 428/2009 submits their trade to the obligation to obtain a license or prior authorization, especially for their export to «sensitive» countries. It may even be prohibited, especially to countries under embargoes. Many sectors are today covered by this regulation. This is mainly due to the quick spread of new technologies, especially in the telecommunication sector.

The Internal Compliance Program, the next standard for dual-use goods.

Unlike the Wassenaar Arrangement¹, European and French regulations on dual-use goods do not require nor encourage exporters to implement Internal Compliance Program (“ICP”).

The issuance of this European practical guide² is part of a wider project to modernize export control, by simplifying procedures, while ensuring its effectiveness. The recast of the 428/2009 Regulation³, undertaken by the European Union, plans to submit export control authorization for large and global projects to the implementation of an ICP by the exporter. Therefore, these ICP guidelines were developed to support companies on key elements to be included in their ICP and how to enforce it. The goal is to ensure effective control of compliance with regulations.

Key elements of an effective IPC

The guidelines provide a framework for companies to identify, manage and comply with the regulations in force. This helps to mitigate risks and violations, and therefore avoid penalties. In this way, this flexible document helps to set up internal principles and procedures for the prevention and control of trade in dual-use goods, adapted to each organization (size, structure, etc.), to the type and complexity of activities (finished product, components, software, services...) and end-users (States, public bodies, private actors...). Seven recommendations are the key elements of an effective ICP:

1. Management Commitment to Compliance
2. Organizational Structure, Responsibilities and Resources
3. Training and awareness
4. Processes and procedures for transaction verification
5. Performance Reviews, Audits, Reports and Corrective Actions
6. Record keeping and documentation
7. Physical security and information security

¹ Signed on May 12th, 1996, the Wassenaar Arrangement brings together 40 States agreeing to subject the export of arms and dual-use goods to a multilateral control and information exchange regime.

² Available here: http://trade.ec.europa.eu/doclib/docs/2018/september/tradoc_157336.pdf.

³ Available here: <https://ec.europa.eu/transparency/regdoc/rep/1/2016/FR/1-2016-616-FR-F1-1.PDF>.