Ministry of Foreign Affairs

Internal Compliance Programme

Guidelines for compiling an Internal Compliance Programme for Strategic Goods, Torture Goods, Technology and Sanctions

Publication date: December 2019

Version 1.2

Foreword

This document contains guidelines for businesses and was drawn up by the Ministry of Foreign Affairs in close collaboration with the Central Office for Import and Export (CDIU). It serves as a guide for implementing an Internal Compliance Programme (ICP) that sets out responsibilities for compliance with the applicable legal requirements. This document is primarily intended for exporters of strategic and sanctioned goods. It also provides useful pointers for exporters of strategic technology.

Dutch export control policy is based on international agreements and commitments that have been implemented at national level on the basis of EU legislation. The Netherlands has signed a number of conventions and takes part in the international export control regimes that aim to regulate the global distribution of certain 'sensitive' goods. The countries participating in these regimes make agreements on export control policy and draw up control lists for the goods in question. Sensitive goods include dual-use and military goods.

Responsibility for ethical export control lies with both the business community and the competent authorities. The Dutch government monitors export control on strategic goods. Detailed information can be found in the *User Guide on Strategic Goods and Services*.[1] An important tool for developing and implementing ethical export control procedures within a company is an ICP.

[1] https://www.government.nl/documents/directives/2012/04/12/user-guide-on-strategic-goods-and-services

Contents

Introduction

An Internal Compliance Programme (ICP) describes the internal control measures required for ensuring compliance with export control laws and regulations. A well thought-out ICP will enhance policy and its implementation within a company's various departments.

It serves as an in-house manual detailing such matters as the internal protocols and procedures put in place to deal with all risks relating to export control. An ICP must always be tailored to a company's individual circumstances. A customised approach is necessary because a company's export control policy depends on a variety of factors. These include the size of the company, the goods in question and the market in which the company operates. Dutch policy sets out a number of basic elements that an ICP should contain. The basic elements of an ICP are described in chapter 1.

A well-implemented ICP has numerous benefits. For instance, it reduces the risk of a company breaking the law and enables it to make use of global licenses. Having a global license reduces the number of separate licenses a company needs to apply for each year, cuts delivery times, provides customers with continuity and reduces the administrative burden. A well-developed ICP helps the Dutch government and the business community fulfil their shared responsibility for preventing the undesirable export of strategic goods. This in turn contributes to international security.

With an ICP a company can demonstrate to the competent authorities that the level of compliance is sufficient. The CDIU checks a company's ICP, identifies any points for improvement and ultimately approves the programme when it covers the required subjects in sufficient detail and that all risks associated with the misuse and diversion of goods are covered.

1. Core elements

An ICP must cover a number of core elements. Below you will find the requirements for each element.

1.1 Commitment to compliance with the legal requirements

A company's top-level management is responsible for promoting and ensuring compliance with the relevant legislation. The management team must actively raise awareness of the company's export control responsibilities, including the risks involved and the importance of compliance with the rules and regulations. Topics to be covered are the importance of export control (to prevent goods from falling into the wrong hands), responsible business conduct and the consequences of violating the law. The statement also explains that dedication from all personnel is expected when it comes to compliance.

It is also important to actively get this message across – for example in the form of a management statement – to staff members who are not directly involved in export control. This will make the entire organisation aware of the subject of export control so that everyone understands why compliance is so important and can see that the management attaches great value to it.

This commitment needs to be renewed on a regular basis by means of new statements, training courses or other activities.

1.2 Structure and responsibility

Responsibility for export control must be embedded in the organisational structure, preferably in a specific department.

If the company's size allows this, it is important to ensure a clear separation of duties in order to prevent conflicts of interest. Export compliance tasks should not, for example, be carried out by a sales department or sales-related department.

One person should be given ultimate responsibility, preferably someone who has or who can gain sufficient knowledge of the subject in order to carry out the task properly. At a minimum, the following tasks need to be assigned within the organisation:

i. compiling and revising the ICP;

ii. drawing up and revising procedures;

iii. keeping track of changes in relevant legislation and changes in the working methods/policy of the competent authorities;

iv. classifying, identifying, screening and approving commercial transactions;

v. performing export control management within the organisation, including guidance/steering and communication;

vi. assigning staff responsible for periodic audits;

vii. training staff.

Larger organisations can choose to designate one member of staff per department/unit as point of contact for export control matters. Regardless of how this is arranged, it is important to ensure that there is sufficient capacity within each part of the organisation to guarantee good compliance.

The ICP should contain a clear description of the company structure, for example in the form of an organisation chart, including the clear separation of duties. It should also list the names, tasks and contact details of the staff responsible for export control and compliance.

1.3 Export screening procedure

The screening procedure must include a number of basic elements.

1.3.1 Classification and identification

All compliant companies are aware of the European and national legal requirements they must comply to. This means that they are able to classify goods themselves and determine whether they require a license. This classification applies not only to goods, but also to, for example, technology and software. Compliant companies also know when sanctions apply, which destinations are classified as sensitive and how to find the relevant rules and regulations.

An ICP should explain the difference between sanctioned and sensitive countries. Companies are responsible for having the knowledge to be able to define sensitive countries for example, by keeping updated on motions filed in the house of representatives, like 'Motie Servaes' or by staying aware of changes within geo-politics or a countries internal situation. The combination of an item and a country of destination can be essential for defining certain risks.

For example:

- Has the country of (final) destination signed the non-proliferation treaty, when nuclear items are involved?;
- What is the human rights situation of the country of (final) destination if cryptography items are involved?

When a country can be defined as sensitive, end user and end use check should be extra thorough (for example in the case the end-user is part of government). It is also a possibility that your company seeks communication about this with the CDIU.

For classification and identification purposes it is essential that the staff responsible are familiar with the relevant legislation and are able to consult it at any time in order to identify any possible changes. This is especially important given that legislation is constantly changing.

The above details need to be set out in the ICP, including references to the applicable legislation and how companies keep track of changes in legislation. One way of describing procedures and processes is to use flowcharts.

The ICP should also explain when a procedure should be started at the CDIU, for example when a license application needs to be submitted, including details of the transaction and/or documents required and the conditions that apply.

1.3.2 Screening consignees, end users and end use

An ICP should describe how the company screens consignees, end users and other parties involved, and how it ensures that no products are supplied to sanctioned parties or parties to which risks (such as diversion of goods) are attached. This screening should include an examination of restricted parties lists, sanction legislation for the country in question, and European and international trade restrictions. The company also needs to investigate whether there are any risks involved in the supply of products, by consulting open sources and for example verify whether the company has a sanctioned parent

company. An automated system or external service can be used for screening purposes. The exporter is responsible for assessing the quality of the sources and systems used.

A red flag checklist is an essential tool for identifying potential risks like diversion. The following questions could be included in the list:

- Can clear information about the end user be found in open sources?
- Does the end user have a physical address and not just a P.O. box, for example?
- Are the customer's business activities clear?
- Has there been any personal contact with representatives of the consignee and/or end user?
- Does the customer want to pay in cash or pay an unreasonable price?
- Are the terms of delivery clear?
- Has the customer filled in an end-use statement correctly and in full?

For all transactions, the end use must be known. The primary aim of export control is to prevent products from being used for the wrong purposes, such as proliferation or human rights violations. Compliant companies have safeguards in place to prevent goods from being used for purposes other than the stated end use.

These safeguards must be set out in the ICP, describing what is being done to prevent goods from being diverted to an undesirable destination. One example is applying certain incoterms.

Having an end-use statement signed by the end-user can cover risks to a certain degree. Validating this end-use statement can offer a further safeguard. The Chamber of Commerce or a similar competent independent organisation can verify whether the company in question exists and is registered, and whether the statements and signatures are authentic.

1.3.3 Supplies to distributors

When supplying to distributors a company needs to have procedures in place to establish that the distributor is also compliant. A distributor must be able to extend the exporter's control to the end user and must comply with all applicable legislation. A company's responsibility stretches beyond the distributor to the end user. End user checks should be done by the company itself, when an order to a new/unknown end-user is placed at the distributor. The distributor can only ship when the company gives permission. This means that the company must be able to establish at all times to which end user the goods have been delivered.

1.3.4 Consulting the competent authorities/ad hoc (catch-all) licensing requirement

Companies need to be aware that they may be subject to an ad hoc licensing requirement and should know in what circumstances this could apply.[2] They should consult the competent authority – the CDIU – in the following and similar cases:

- if there is any doubt about the end use and/or end user;
- if they have prior knowledge or doubts about the diversion of the goods;

[2] Article 4 - Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

- if information about any of the parties involved raises questions.

Companies must also be aware that non-controlled goods may not be exported to sanctioned entities if they are intended for military end use.

1.4 Shipment control

Before actually shipping the items, companies must do a last check whether all aspects of the implemented procedures have been carried out correctly and whether the export declaration complies with the required legal formalities. This means among other things, companies should check whether end-users are actually screened and whether the obtained license is still valid.

There are several ways of doing this. One example is to use an automated system that deploys a stop-hold-release procedure that can hold transactions so that they can be verified by an authorised person in the case of irregularities.

1.5 Training

As noted above, it is essential that the entire organisation is aware of export control requirements. New staff who will be involved in export control tasks need to be tested to ensure they have sufficient knowledge of the field. When necessary they should be offered training to bring their knowledge up to the required level. New staff also need to be familiarised with the company's export control processes and protocols. It is important to provide regular training to all staff involved in export control, to ensure they expand their knowledge where necessary and stay up to date. A record should be kept of the courses each staff member has taken.

The ICP should describe how staff are trained and gain experience in these tasks.

1.6 Audits, reporting and improvement measures

In order to assess their level of compliance, companies need to carry out an internal audit at least once a year, and preferably have periodic audits carried out by an independent external party. The aim of these audits is to establish whether export control is being properly implemented in accordance with the ICP. Part of the audit is to check whether the ICP is up to date and the company is still compliant.

If it emerges from an audit that aspects of the ICP have been insufficiently or incorrectly implemented or safeguarded, the company must launch an improvement process. The process and its outcome should be reported to the top level management.

If an audit identifies a possible violation of export control laws or methods, the company can opt to report this to the CDIU by means of a Voluntary Self-Disclosure.

Any changes made to working methods need to be recorded in the ICP. Revised versions of the ICP should be sent as soon as possible to the CDIU.

1.7 Archiving

All export-related documents must be retained for seven years, in accordance with the statutory requirements. The competent authorities must be able to request documents from the archives at all times.

2. Supplementary sections on controlled technology, cyber surveillance and torture goods

In addition to the core elements, companies that deal with controlled technology, cyber surveillance or potential torture goods also need to include information on these activities in their ICP.

2.1 Exporting controlled technology

Trade controls for dual-use items include software and technology. The export of controlled technology can be broken down into two categories:

1. Tangible export of technology includes but is not limited to the transfer of, for example, construction blueprints, scientific publications or technology by means of electronic data carriers, etc.;
2. Intangible export of knowledge, also known as intangible technology transfer (ITT), entails the transfer of technology by word of mouth or through practices learned, e-mail, transfer via the cloud, etc. that is not subject to the knowledge embargo referred to in the sanctions regulations.

Please note: Technology transfer is subject to a licensing requirement as soon as the technology (as defined in the General Technology Note) leaves the EU. This also applies to intra-company transfers. In the case of nuclear technology (as defined in the Nuclear Technology Note), technology transfer is subject to a licensing requirement as soon as the technology leaves the Netherlands.

It is important to prevent unauthorised access to or removal of controlled dual-use technology by employees or third parties. Therefore, it is important to take the necessary security measures to make sure that the risks on unauthorised removal of or access to the technology are limited. These are both physical security and information security measures.

If a company has a global license to export technology, the ICP must explain how the company ensures that exports are not subject to, for example, proliferation risks. This includes details of how the company ensures that information is supplied to the intended end users only, that these are screened in accordance with the standard procedure and that the company has a good overview of the exported technology at all times.

The ICP must contain information on at least the following points:

- Measures against unauthorised removal of or access to the tangible dual-use technology by employees or third parties. An example is introducing restrictions on the access to areas and employees so only authorised personnel can access the dual-use technology;

- Measures and procedures for secured storage of and access to controlled intangible dual-use technology, including antivirus checks, file encryption, audit trails and log, user access control and firewall.

2.2 Cyber surveillance and human rights

The Netherlands, EU and UN alike attach great importance to respect for human rights. The Dutch government wants to prevent goods exported from Europe being used for purposes associated with the violation of human rights, democratic principles or freedom of expression, as described in the Charter of Fundamental Rights of the European Union. Goods falling into categories 4 and 5 of the Dual-use Regulation (EC No 428/2009) in particular can be used for such purposes.

The Dutch government has excluded a number of countries where there are concerns about potential human rights violations from global licenses. This list of countries is dynamic and its composition depends on the global geopolitical situation. In addition to the excluded countries, there are also countries where the risks are not as high but where transactions of the goods in question still require careful monitoring, for example goods being sent to a government authority.

When implementing procedures relating to human rights, it is above all important to raise awareness and acquire knowledge.[3] This includes knowledge about how the goods to be delivered could be used for purposes that violate human rights, and about which countries require extra vigilance. Further checks can then be carried out on, for example, a country's political situation and the role the end user plays in it. An additional declaration/condition relating to this should be included in the end-use statement.

The ICP must contain information on at least the following points:

- the management's vision on this subject;
- whether and, if so, how the goods being supplied could be used in the violation of human rights or indeed in the protection of human rights, for example through the encryption of certain data;
- clear awareness of specific regions and countries for which additional checks are required and awareness of the fact that the situation is constantly changing;
- special focus on supplies to certain government authorities (in particular police forces, armed forces and intelligence and security services) and supplies to telecom providers and/or data storage providers which may be obliged to take part in practices that violate human rights;
- extra procedures put in place to prevent goods being used for the purposes in question;
- how the company ensures that it stays informed of the latest news and policy changes and communicates this information to staff;
- at what point the company would consult the competent authorities if doubts should arise.

[3] Relevant sources include the 'Guiding Principles on Business and Human Rights', the 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', the Digital Agenda for Europe, UN human rights reports, information from NGOs (such as Privacy International, Freedom House, OpenNet Initiative) and research institutes such as CitizenLab.

2.3 Torture goods

The Charter of Fundamental Rights of the European Union contains the basic principles for prohibiting the death penalty, torture, or other inhuman or degrading treatment or punishment. The anti-torture regulation (EC No 2019/125) provides the legal basis for provisions regarding the export of goods that could potentially be used for the purposes stated above.

In order to comply with the law it is important to raise awareness and acquire knowledge of such practices. This includes knowledge about how goods to be delivered could be used to carry out the death penalty, torture or other cruel, inhuman or other degrading treatment or punishment, and which countries require extra vigilance. Procedures for the export of such goods will need to be implemented and extra checks carried out on, for example, a country's political situation and the role the end user plays in it. An additional declaration/condition relating to this should be included in the end-use statement

The ICP must contain information on at least the following points:

- the management's vision on this subject;
- clear awareness of specific regions and countries for which additional checks are required, for example countries that still impose the death penalty;
- special focus on supply of goods to certain government authorities (in particular prisons);
- extra procedures to prevent goods from being used to carry out the death penalty, torture or other cruel, inhuman or degrading treatment or punishment;
- how the company ensures that it stays informed of the latest news and policy changes and communicates this to staff;
- a focus on consulting the competent authorities in case of doubt.

Appendix I: Information and sources

This appendix contains sources of information about compliance that can be consulted. This is not an exhaustive list. It remains the responsibility of the company to maintain a complete list of sources and identify changes and new sources. Please ensure that you always consult the most recent version.

A. Legislation

Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

Strategic Services Act of 29 September 2011, containing rules concerning the control of services relating to strategic goods

Strategic Services Implementing Regulations; Order of the State Secretary for Economic Affairs, Agriculture and Innovation of 7 November 2011, no. WJZ / 11158559, containing rules concerning the implementation of the Strategic Services Act

Strategic Goods Decree of 24 June 2008, containing rules concerning the import, export and transit of dual-use and military goods

Strategic Goods Implementing Regulations 2012; Order of the State Secretary for Economic Affairs, Agriculture and Innovation of 28 October 2011, no. WJZ / 11134677, laying down revised implementing regulations on strategic goods

Guidance notes on *the Strategic Services Act and the Strategic Services Implementing Regulations;* memo no. BEB/HPG/12015427; Directorate-General for International Relations; 22 August 2012

Ministerial order on dual-use goods; Order of the Minister for Foreign Trade and Development Cooperation of 9 September 2013, no. DJZ/BR/0648-2013, concerning a licensing requirement for the export of and provision of brokerage services for dual-use goods

Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community

Council Regulation (EC) No 2019/125 of 16 January 2019 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment

B. Sanctions legislation

Applicable EU restrictive measures (sanctions):
https://www.rijksoverheid.nl/documenten/rapporten/2014/04/23/sanctieregelingen-actuele-stand-van-zaken (in Dutch)

http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf

https://www.sanctionsmap.eu/#/main

Council Regulation (EU) No 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010

Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010

Ukraine Territorial Integrity Sanctions Order 2014; Order of the Minister of Foreign Affairs of 19 March 2014, no. MinBuZa.2014.119597, containing restrictive measures concerning actions that undermine or threaten the territorial integrity, sovereignty and independence of Ukraine

Council Regulation (EU) No 36/2012 of 18 January 2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011

Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007

Motion by MP Michiel Servaes regarding Saudi Arabia: https://zoek.officielebekendmakingen.nl/kst-22054-273.html (in Dutch)

C. Background information

User Guide on Strategic Goods and Services, Ministry of Foreign Affairs , July 2013

Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies, Wassenaar Arrangement

Principles and Examples of Good Practices, Nuclear Suppliers Group

Strengthening Strategic Export Controls by Internal Compliance Programmes – Joint Research Centre report
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC92964/sevini%20-%20online.pdf

OECD Guidelines
https://www.oecdguidelines.nl/

D. Human rights

http://www.minbuza.nl/ecer/eu-essentieel/handvest-grondrechten (in Dutch)

Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council preparatory bodies; Council of the European Union; Brussels, 20 January 2015

UN Guiding Principles on Business and Human Rights; Implementing the United Nations 'Protect, Respect and Remedy' Framework; United Nations Human Rights Office of the High Commissioner; New York and Geneva, 2011

ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights; Shift and the Institute for Human Rights and Business; European Commission, 2013

The European Union Explained, Digital Agenda for Europe: Rebooting Europe's Economy; Luxembourg; Publications Office of the European Union, 2014

https://freedomhouse.org/

https://www.privacyinternational.org/

https://opennet.net/

E. Other

https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/douane_voor_bedrijven/veiligheid_gezondheid_economie_en_milieu_vgem/cdiu/centrale_dienst_in_en_uitvoer_cdiu
(in Dutch)

This is a publication by:

Ministry of Foreign Affairs

Postbus 20061 | 2500 EB Den Haag