RECOMMENDATIONS

COMMISSION RECOMMENDATION (EU) 2019/1318

of 30 July 2019

on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Article 19(5) of 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 ([1]),

Whereas:

(1) Regulation (EC) No 428/2009 sets up a Union regime for the control of exports, transfer, brokering and transit of dual-use items.

(2) An effective, uniform and consistent system of export controls on dual-use items is necessary to promote EU and international security and to ensure both compliance with the international commitments and responsibilities of the Member States and of the European Union (EU), especially regarding non-proliferation, and the promotion of a level playing fields among EU operators.

(3) Common approaches and practices as regards internal compliance programmes can contribute to a uniform and consistent application of controls throughout the EU.

(4) Taking into consideration rapid scientific and technological advancements and the complexity of today's supply chains, effective trade controls depend to a great extent on the awareness of exporters and their active efforts to comply with trade restrictions. To this end, companies usually put in place a set of internal policies and procedures, also known as an Internal Compliance Programme (ICP).

(5) This guidance provides a framework to help exporters identify, manage and mitigate risks associated with dual-use trade controls and to ensure compliance with the relevant EU and national laws and regulations.

(6) This guidance also provides a framework to support Member States competent authorities in their assessment of risks, in the exercise of their responsibility for deciding on individual, global or national general export authorisations, on authorisations for brokering services, on transits of non-Community dual-use items or on authorisations for the transfer within the Community of the dual-use items listed in Annex IV of Regulation (EC) No 428/2009.

(7) This guidance should be non-binding and exporters shall maintain the responsibility to comply with their obligations under the Regulation, while the Commission should ensure that this guidance remains relevant over time,

([1]) OJ L 134, 29.5.2009, p. 1.

HAS ADOPTED THIS RECOMMENDATION:

Member States competent authorities and exporters under Regulation (EC) No 428/2009 should consider the non-binding guidance provided in the Annex to this Recommendation in order to fulfil their obligations under that Regulation.

Done at Brussels, 30 July 2019.

For the Commission
Cecilia MALMSTRÖM
Member of the Commission

ANNEX

EU GUIDANCE ON INTERNAL COMPLIANCE PROGRAMME (ICP) FOR DUAL-USE TRADE CONTROLS

INTRODUCTION

Effective controls on trade in dual-use items — goods, software and technology — are vital for countering risks associated with the proliferation of Weapons of Mass Destruction (WMD) and the destabilising accumulations of conventional weapons. Companies dealing with dual-use items are obliged to comply with strategic trade control requirements imposed under the laws and regulations of the European Union ([1]) and its Member States. They need to refrain from participating in transactions where there are concerns that items may be used for proliferation purposes.

Taking into consideration rapid scientific and technological advancements, the complexity of today's supply chains and the ever growing significance of non-State actors, effective trade controls depend to a great extent on the awareness of 'companies' ([2]) and their active efforts to comply with trade restrictions. To this end, companies usually put in place a set of internal policies and procedures, also known as an Internal Compliance Programme (ICP), to ensure compliance with EU and national dual-use trade control laws and regulations. The scope and the extent of these policies and procedures are usually determined by the size and the commercial activities of the specific company.

In order to support companies to maintain strict compliance with the relevant EU and national laws and regulations, this guidance provides a framework to identify and manage dual-use trade controls' impact and mitigate associated risks. The guidance focuses on the 7 core elements for an effective ICP. Each core element is further detailed by a section 'What is expected' that describes the objective(s) of each core element, and a section 'What are the steps involved?' that further specifies the actions and outlines possible solutions for developing or implementing compliance procedures. This document concludes with a set of helpful questions pertaining to a company's ICP and a list of diversion risk indicators and 'red flag' signs about suspicious enquiries or orders.

The development of EU ICP guidance for dual-use trade controls takes into consideration and builds on existing approaches to export control compliance, and in particular:

— the 2011 Wassenaar Arrangement Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies ([3]),

— the 'Best Practice Guide for Industry' from the Nuclear Suppliers Group (NSG) ([4])

— the ICP elements in the Commission Recommendation 2011/24/EU ([5]),

— the results from the fourth Wiesbaden Conference (2015) on 'Private Sector Engagement in Strategic Trade Controls: Recommendations for Effective Approaches on United Nations Security Council Resolution 1540 (2004) Implementation'

— the 2017 United States Export Control and Related Border Security Program ICP Guide website ([6]).

The guidance contains 7 core elements that should not be considered as an exhaustive list, nor should their order be perceived as ranking from very important to less important. They are identified as cornerstones for a company's tailor-made ICP and aim at assisting companies in their reflections on the most appropriate means and procedures for compliance with EU and national dual-use trade control laws and regulations. Affected companies are expected to have a range of existing policies and processes in place in relation to export control. For these companies, the core elements' structure could facilitate benchmarking their compliance approach. A company's approach to compliance that includes

([1]) Regulation (EC) No 428/2009.
([2]) For the purpose of this document, the term 'companies' should be understood in a broad sense. It includes research, academic and other entities qualifying as 'exporters' under Regulation (EC) No 428/2009. This guidance does not provide (at this stage) specific advice for the different sectors and actors involved.
([3]) See also https://www.wassenaar.org/app/uploads/2015/06/2-Internal-Compliance-Programmes.pdf
([4]) See also http://www.nuclearsuppliersgroup.org/images/Files/National_Practices/NSG_Measures_for_industry_update_revised_v3.0.pdf
([5]) Commission Recommendation 2011/24/EU of 11 January 2011 on the certification of defence undertakings under Article 9 of Directive 2009/43/EC of the European Parliament and of the Council simplifying terms and conditions of transfers of defence-related products within the Community (OJ L 11, 15.1.2011, p. 62).
([6]) See also http://icpguidelines.com

policies and internal procedures for, at least, all the core elements could be expected to be in line with the EU ICP guidance for dual-use trade controls. For companies that are in the process of developing a compliance approach for dual-use trade, the core elements' structure offers a basic and generic skeleton for company compliance.

At a general level, the most important aspect of developing an ICP, is to keep it relevant to the company's organisation and activities, and to make sure that internal processes are easy to understand and follow, and capture the day-to-day operations and procedures. The individual requirements and characteristics of an ICP will depend on the size, structure and scope of the company's specific business activity, but also on the strategic nature of its items and possible end-uses or end-users, on the geographic presence of its customers and on the complexity of internal export processes. Therefore, it is important to stress that, during the development of this guidance, potential implementation challenges for Small and Medium Sized Enterprises (SMEs) were systematically considered.

Disclaimer

This guidance is of a non-binding character and should not to be considered as legal advice. This guidance is without prejudice to the decisions on authorisations, that are the responsibility of the competent authorities under Regulation (EC) No 428/2009.

In case you wish to share feedback on the content of this document, please contact your competent authority (see Annex 3).

EU ICP GUIDANCE FOR DUAL-USE TRADE CONTROLS

The following core elements are essential for an effective dual-use trade control Internal Compliance Programme:

1. Top-level management commitment to compliance

2. Organisation structure, responsibilities and resources

3. Training and awareness raising

4. Transaction screening process and procedures

5. Performance review, audits, reporting and corrective actions

6. Recordkeeping and documentation

7. Physical and information security

For each core element, the section '**What is expected?**' describes the ICP related objective(s). The section '**What are the steps involved?**' further specifies the actions and outlines possible solutions for developing or implementing compliance procedures.

With this in mind, the core elements should be understood as 'building blocks' for the preparation of ICPs by companies involved in dual-use trade. Each company should describe within its own tailor-made ICP how it implements the relevant core elements in consideration of its specific circumstances.

In doing so, all companies involved in dual-use trade should consider in particular the actions contained in the section '**What are the steps involved**', though companies may deviate from these actions if there are company-specific reasons for doing so.

RISK ASSESSMENT

An ICP needs to be tailored to the size, the structure and scope of the business, and, especially, to the company's specific business activity and related risks. Therefore, if a company wants to develop or review its compliance programme for dual-use trade control, it is recommended to start with a risk assessment to determine its specific dual-use trade risk profile. It will help the company to become aware of what parts of its business need to be covered by the ICP and target the ICP to the company's specific circumstances.

The risk assessment should carefully assess the product range, customer base and business activity that are or could be affected by dual-use trade control. It should identify relevant vulnerabilities and risks so that the company can incorporate ways to mitigate them under the ICP. Even though this risk assessment cannot identify all vulnerabilities and risks your company may face in future, it will give the company a better base to develop or review its ICP.

Companies often already have internal control processes in place and therefore, do not need to start from scratch when designing ICPs. The risk assessment supports a company to assess its existing corporate policies and procedures against export control related risks and come up with a course of action for adapting them, if necessary. In addition, promoting synergies between existing policies and export control requirements is a further step to consider from the beginning. For instance, it is a good practice to insert cross references to export control principles and requirements in the company's code of conduct, if available.

The outcomes of this risk assessment will affect the necessary actions and appropriate solutions for developing or implementing the company's specific compliance procedures.

A company may try to benefit as much as possible from the advantages of global, group-wide ICP solutions, but must always comply with all applicable EU and Member State laws and regulations.

AUTHORISED ECONOMIC OPERATOR ([7])

If a company holds of a valid Authorised Economic Operator (AEO) authorisation, the assessment of the company's compliance covering relevant customs activities could be taken into account for the purpose of developing or reviewing an ICP.

Taking into consideration that customs authorities have checked the customs routines and procedures of your company, the AEO status could be an asset for establishing or reviewing procedures relating to ICP core elements such as record-keeping and physical security.

1. **Top-level management commitment to compliance**

Effective ICPs reflect a top-down process whereby the company's top-level management gives significance, legitimacy, and organisational, human and technical resources for the corporate compliance commitments and compliance culture.

What is expected?

Top-level management commitment aims to build compliance leadership (lead by example) and corporate compliance culture for dual-use trade control.

A written statement of support to internal compliance procedures by the top-level management promotes the company's awareness of the objectives of dual-use trade controls and compliance with the relevant EU and Member State laws and regulations.

The commitment indicates clear, strong and continuous engagement and support by top-level management. It results in sufficient organisational, human and technical resources for the company's commitment to compliance. The management communicates clearly and regularly to employees about the corporate commitment in order to promote a culture of compliance.

What are the steps involved?

Develop a corporate commitment statement stating that the company complies with all EU and Member State dual-use trade control laws and regulations.

([7]) See also https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/authorised-economic-operator-aeo_en

Define the management's specific compliance expectations and convey the importance and value placed on effective compliance procedures ([8]).

Clearly and regularly communicate the corporate commitment statement to all employees (also employees with no role in dual-use trade control) in order to promote a culture of compliance ([9]).

2. **Organisation structure, responsibilities and resources**

Sufficient organisational, human and technical resources are essential for effectively developing and implementing compliance procedures. Without a clear organisation structure and well-defined responsibilities, an ICP risks suffering from lack of oversight and undefined roles. Having a strong structure helps organisations work out problems when they arise and prevent unauthorised transactions from occurring.

What is expected?

The company has an internal organisational structure that is set down in writing (for instance in an organisational chart) and that allows for conducting internal compliance controls. It identifies and appoints the person(s) with the overall responsibility to ensure the corporate compliance commitments. Please be aware that in some Member States this must be a member of the top-level management.

All compliance related functions, duties and responsibilities are defined, assigned and connected to each other in an order that ensures the management that the company conducts overall compliance. Where appropriate or even necessary, functions and/or duties relating to export controls (but not the overall responsibility) may be delegated within the entity or shared between two or more corporate entities within the EU.

The company adequately staffs all areas of the business that are related to dual-use trade with employees who demonstrably have the required skills. At least one person in the company is (not necessarily exclusively) entrusted with a dual-use trade control function. This function can be shared between corporate entities within the EU as long as an appropriate level of controls is maintained. Please note however that in some EU Member States this may not be possible, as national export control legislation requires a dedicated person to be appointed locally.

Dual-use trade control staff should be protected as much as possible from conflicts of interest. This staff is entitled to directly report to the person(s) with the overall responsibility for dual-use trade controls and should additionally have the power to stop transactions.

Dual-use trade control staff must have access to the relevant legislative texts, including the latest lists of controlled goods and lists concerning embargoed or sanctioned destinations and entities. Appropriate operational and organisational processes and procedures, relevant for dual-use trade controls, are documented, gathered and distributed to all relevant personnel.

The company should have a compilation of the documented processes and procedures (e.g. in a compliance manual) that is up-to-date. Depending on its size and its business volume, the company should consider the need for IT support for internal compliance procedures.

What are the steps involved?

Determine the number of dual-use trade control staff, taking into account legal and technical aspects which need to be covered. Entrust at least one person in the company with the company's dual-use trade compliance and ensure that an equally qualified substitute can assume the task in case of absence (such as sickness, holiday and so on). Depending on the average volume of orders, this person may only have to handle tasks relating to dual-use export control on a part-time basis.

([8]) The corporate commitment statement could, for example, state that under no circumstances exports, brokering, transit or transfer can be made contrary to EU and Member State dual-use trade control laws and regulations by any individual operating on behalf of the company. In order to strengthen the understanding of the necessity of export controls, the statement may briefly explain their objectives. It could also stress the importance of employees being compliant with export controls, so that the employees understand possible non-compliance scenarios by communicating the risks of unauthorised transactions and possible consequences (criminal, reputational, financial, disciplinary etc.) for the company and the involved employees. It is recommended to keep the management commitment to compliance as simple as possible.

([9]) Companies could also consider disseminating the statement publicly through corporate websites and other commercial channels to inform third parties of the company's commitment to export control compliance.

Clearly identify, define and assign all compliance related functions, duties and responsibilities, possibly in an organisational chart. Clearly identify back-up functions whenever possible.

Make sure that the internal organisational structure for dual-use trade control is known throughout the organisation and that the internal records of these assignments are routinely updated and distributed to employees. Make the contact details of the responsible person for dual-use trade control questions known within the company. If trade control duties are being outsourced, the interface to and the communication with the company needs to be organised.

Define the knowledge and skills needed by legal and technical dual-use trade control staff. Job descriptions are recommended.

Make sure that dual-use trade control staff is protected as much as possible from conflicts of interest. Depending on the size of the company, the responsibility for compliance may be laid down at a suitable department or division. For example: person(s) making the final decision whether goods can be shipped, are not part of the sales department, but part of the legal department. Allow this staff to function as expert advisors to guide company decisions resulting in compliant transactions.

Document and distribute the set of policies and procedures addressing dual-use trade controls to all relevant personnel.

Compile the documented policies and procedures and consider the format of a compliance manual.

3. **Training and awareness raising**

Training and awareness raising on dual-use trade control is essential for staff to duly perform their tasks and take compliance duties seriously.

What is expected?

The company ensures via training that the dual-use trade control staff is aware of all relevant export control regulations as well as the company's ICP and all amendments to them. Examples of training material are external seminars, subscription to information sessions offered by competent authorities, in-house training events, and so on.

Furthermore, the company carries out awareness raising for the employees at all relevant levels.

What are the steps involved?

Provide compulsory, periodic training for all dual-use trade control staff to ensure they possess the knowledge to be compliant with the regulations and the company's ICP.

Ensure via training that all concerned employees are aware of all relevant dual-use trade control laws, regulations, policies, control lists and all amendments to them as soon as they are made public by the competent authorities. If possible, consider customised trainings.

Develop general awareness raising for all employees and dedicated training activities for e.g. purchasing, engineering, project management, shipping, customer care and invoicing.

Consider, whenever appropriate, to make use of national or EU training initiatives for dual-use trade control.

Incorporate lessons learnt from performance reviews, audits, reporting and corrective actions, whenever possible, in your training or export awareness programs.

4. **Transaction screening process and procedures**

In terms of operational implementation, transaction screening is the most critical element of an ICP. This element contains the company's internal measures to ensure that no transaction is made without the required license or in breach of any relevant trade restriction or prohibition.

The transaction screening procedures collect and analyse relevant information concerning item classification, transaction risk assessment, license determination and application, and post-licensing controls.

Transaction screening measures also allow the company to develop and maintain a certain standard of care for handling suspicious enquiries or orders.

What is expected?

The company establishes a process to evaluate whether or not a transaction involving dual-use items is subject to national or EU dual-use trade controls and determine the applicable processes and procedures. In case of recurring transactions, transaction screening needs to be performed periodically.

This core element is divided into:

— Item classification, for goods, software and technology;

— Transaction risk assessment, including

  — Checks on trade-related embargoed, sanctioned or 'sensitive destinations and entities' ([10]);

  — Stated end-use and involved parties screening;

  — Diversion risk screening;

  — 'Catch-all controls' for non-listed dual-use items;

— Determination of license requirements and licence application as appropriate, including for brokering, transfer and transit activities; and

— Post-licencing controls, including shipment control and compliance with the conditions of the authorisation.

In case of doubt or suspicion during the transactions screening process, in particular about the results of the stated end-use and involved parties or diversion risk screening, please consult with the competent authority in the EU Member State where your company is established.

Transaction screening can be done manually or with the support of automated tools, depending on your company's needs and available resources.

What are the steps involved?

Item classification

Item classification is about determining whether the items are listed. This is done by comparing the technical characteristics of an item against the EU and national dual-use control lists. If applicable, identify whether the item is subject to restrictive measures (including sanctions) imposed by the EU or the EU Member State in which your company is established.

Understand that dual-use items, whether a physical product, software or technology, could require a license for various reasons.

Pay particular attention to the classification of dual-use components and spare parts, and to the classification of dual-use software and technology that can be transferred by email or made available via, for instance, a 'Cloud' service abroad.

Gather information about the possible misuse of your dual-use items in the context of e.g. conventional military or WMD proliferation. Share this information within the company.

It is recommended to request information from your supplier(s) about the dual-use classification of materials, components, subsystems that are processed or integrated by your company, including machinery used in the production. It is still your company's responsibility to check the classification received from the supplier(s).

([10]) So-called 'sensitive destinations and entities' are not only embargoed or sanctioned destinations, but also other destinations to which the shipment of (certain) dual-use items can be critical in specific cases, for example because of WMD proliferation or human rights concerns, as determined by the competent authority. Concerning human rights concerns, please note that other Regulations may apply, e.g. Regulation (EU) 2019/125 of the European Parliament and of the Council (OJ L 30, 31.1.2019, p. 1) that introduces controls on the export of goods that could be used for capital punishment or for torture.

As required by Article 22(10) of the EC dual-use Regulation (EC) No 428/2009, mention — with a reference to the relevant legislation — in the commercial documents relating to intra-EU-transfers that the transaction involves listed dual-use items and are subject to controls if exported from the EU.

Transaction risk assessment

Checks on embargoed, sanctioned or sensitive destinations and entities

Ensure that none of the involved parties (intermediaries, purchaser, consignee or end-user) are subject to restrictive measures (sanctions) by consulting the up-to-date sanctions lists ([11]).

Stated end-use and involved parties screening;

Know your customers and their end-use of your products.

Consult the information provided by your competent authority for EU and national rules and requirements concerning end-use statements. Even without a national obligation to submit a correctly filled-out and signed end-use statement, an end-use statement may be a useful means to check the reliability of the end-user/consignee and the information can be used to determine if an authorisation is required for non-listed dual-use items where there are stated end-use concerns under the terms of Article 4 of Regulation (EC) No 428/2009 ([12]).

Be vigilant for diversion risk indicators and signs about suspicious enquiries or orders e.g. assess if the stated end-use is consistent with the activities and/or markets of the end-user. Annex 2 contains a list of questions to support stated end-use and involved parties screening.

Diversion risk screening

Be vigilant for diversion risk indicators and signs about suspicious enquiries or orders. Annex 2 contains a list of questions to support diversion risk screening.

Pay particular attention to the catch-all controls for non-listed dual-use items, if the stated end-use and involved parties screening or the diversion risk screening provide information of concern under the terms of Article 4 of Regulation (EC) No 428/2009.

'Catch-all' controls for non-listed dual-use items

Ensure that the company has procedures in place to determine if it is 'aware' that there is information of concern about the stated end-use (under the terms of Article 4 of Regulation (EC) No 428/2009). If the exporter is 'aware', the company ensures that no export occurs without notifying the competent authority and without having received the competent authority's final decision.

For cases in which the exporter is being 'informed' by the competent authorities that there is information of concern about the stated end-use (under the terms of Article 4 of Regulation (EC) No 428/2009), then the company needs to have procedures in place to ensure the swift flow of information and the immediate stop of the export. It must be ensured that the export does not occur without having received an authorisation by the competent authority.

License determination and application, including for brokering, transfer and transit activities

Ensure that your company has the contact details of the competent export control authority.

Gather and disseminate information about the range of license types (including individual, global and general licenses) and controlled activities (including export, brokering, transfer and transit), and about the license application procedures relating to the applicable EU and national dual-use trade controls.

([11]) The consolidated EU sanctions list (https://eeas.europa.eu/topics/sanctions-policy/8442/consolidated-list-sanctions_en) as well as the EU Sanctions Map (https://www.sanctionsmap.eu) may provide assistance in carrying out the sanctions screening.

([12]) In case your customer is unfamiliar with the request for an end-use statement, consider drafting a (one-page) accompanying letter explaining the very basics of dual-use trade controls and indicating that the requested document speeds up applying for a licence or might even be necessary for receiving a license.

Be aware of less obvious controlled types of export (such as export via the 'Cloud' or via a person's personal baggage) and of dual-use trade control measures for activities other than export, such as technical assistance or brokering.

Post-licencing controls, including shipment control and compliance with the conditions of the authorisation

Before the actual shipment, there should be a final check that all steps ensuring compliance were duly taken. This is a good moment to check if items are correctly classified, if 'red flags' have been identified, if the screening of entities was effectively performed and if there is a valid licence for the shipment.

A final transaction risk assessment is necessary in case of a change of relevant legislation in the meantime, for example if the commodity is now a listed dual-use item or the end-user is now sanctioned.

Implement a procedure in which items can be stopped or put on hold when any of the requirements are not met, or when any 'red flags' are raised. The items should only be released by a person with responsibility for compliance.

Ensure that the terms and conditions of the licence have been complied with (including reporting).

Be aware that any changes to the exporting company's details (such as name, address and legal status), to the details of the end-user and/or intermediaries and to the details of the authorised items may affect the validity of your license.

5. **Performance review, audits, reporting and corrective actions**

An ICP is not a static set of measures and therefore must be reviewed, tested and revised if proven necessary for safeguarding compliance.

Performance reviews and audits verify whether the ICP is implemented to operational satisfaction and is consistent with the applicable national and EU export control requirements.

A well-functioning ICP has clear reporting procedures about the notification and escalation actions of employees when a suspected or known incident of non-compliance has occurred. As part of a sound compliance culture, employees must feel confident and reassured when they raise questions or report concerns about compliance in good faith.

Performance reviews, audits and reporting procedures are designed to detect inconsistencies to clarify and revise routines if they (risk to) result in non-compliance.

What is expected?

The company develops performance review procedures to verify the day-to-day compliance work within the company and to check whether the export control operations are implemented appropriately according to the ICP. Performance review is executed internally, enables the early detection of instances of non-compliance and the development of follow-up measures for damage control. Performance review thus reduces risks for the company.

The company has procedures in place for audits, being systematic, targeted and documented inspections to confirm that the ICP is correctly implemented. Audits can be performed internally or by qualified external practitioners.

Reporting is the set of procedures for dual-use trade control staff and other relevant employees regarding the notification and escalation measures to take in the event of suspected or known incidents of dual-use trade non-compliance. It does not refer to external reporting obligations, e.g. in case your company is registered for the use of a union general export authorisation under the terms of Regulation (EC) No 428/2009.

Corrective actions are the set of remedial actions to guarantee the proper implementation of the ICP and the elimination of identified vulnerabilities in the compliance procedures.

What are the steps involved?

Provide for random control mechanisms as part of daily operations to monitor the trade control workflow within the company to ensure that any wrongdoings are detected in an early stage. Another approach is to use the 'four eyes principle', where trade control decisions are reviewed and double-checked.

Develop and perform audits to check the design, adequacy and efficiency of the ICP.

Make sure to include all aspects of the internal compliance programme into the audit.

Ensure that employees feel confident and reassured when they raise questions or report concerns about compliance in good faith.

Establish whistleblowing and escalation procedures to govern the actions of employees when a suspected or known incident of dual-use trade non-compliance has occurred. Third parties may be given this option as well.

Document any suspected breaches of national and EU dual-use control legislation and the associated corrective measures in writing.

Take effective corrective actions to adapt the export control operations or the ICP according to the findings of the performance review, the ICP system audit or the reporting. It is recommended to share these findings, including the revision to procedures and corrective actions with dual-use trade control staff and management. Once the corrective actions have been implemented, it is recommended to communicate the amended procedures to all employees concerned.

A dialogue with your competent authority can contribute to damage control and possible ways to strengthen the company's export control.

6. **Recordkeeping and documentation**

Proportionate, accurate and traceable recordkeeping of dual-use trade control related activities is essential for your company's compliance efforts. A comprehensive recordkeeping system will help your company with conducting performance reviews and audits, complying with EU and/or national documentation retention requirements and it will facilitate cooperation with competent authorities in case of a dual-use trade control enquiry.

What is expected?

Recordkeeping is the set of procedures and guidelines for legal document storage, record management and traceability of dual-use trade control related activities. Recordkeeping of some documents is required by law but it may also be in your company's best interest to keep records of some other documents (e.g. an internal document describing the technical decision to classify an item). Where all required records are captured and correctly filed, this allows for more efficient search and retrieval during the day-to-day dual-use trade control activities, and also during the periodic audits.

What are the steps involved?

Verify the legal requirements for recordkeeping (period of safekeeping, scope of documents, etc.) in the relevant EU and national legislation of the EU Member State where the company is established.

In order to make sure that all relevant documentation is at hand, consider determining the record retention requirements in contracts with intermediaries, including freight forwarders and distributors.

Create an adequate filing and retrieval system for dual-use trade control. Both for paper and electronic systems, performant indexing and search functionalities are essential.

Ensure that export control related documents are maintained in a consistent manner and can be made available promptly to the competent authority or other external parties for inspections or audits.

It is recommended to keep a record of past contacts with the competent authority, also in relation with end-use(r) controls for non-listed dual-use items and in case of technical classification advice.

7. **Physical and information security**

Trade controls for dual-use items, including software and technology, occur for reasons of (inter)national security and foreign policy objectives. Due to their sensitivity, therefore dual-use items should be 'protected', and having appropriate security measures contributes to containing the risks of unauthorised removal of, or access to, controlled items. Physical security measures are important but, because of the very nature of controlled software or technology in electronic form, ensuring compliance with dual-use trade regulations can be particularly challenging and also requires information security measures.

What is expected?

Physical and information security refers to the set of internal procedures that are designed to ensure the prevention of unauthorised access to or removal of dual-use items by employees, contractors, suppliers or visitors. These procedures cultivate a security culture within the company and ensure that dual-use items, including software and technology, do not get lost, are not easily stolen or exported without a valid license.

What are the steps involved?

Physical security

Ensure, according to the company's risk assessment, that controlled dual use items are secured against unauthorised removal by employees or third parties. Measures that could be considered include, for example, physically safeguarding the items, the establishment of restricted access areas and personnel access or exit controls.

Information security

Establish basic safeguarding measures and procedures for secured storage of and access to controlled dual-use software or technology in electronic form, including antivirus checks, file encryption, audit trails and logs, user access control and firewall. If applicable to your company, consider protective measures for uploading software or technology to the 'Cloud', storing it in the 'Cloud' or transmitting it via the 'Cloud'.

Annex 1

Helpful questions pertaining to a company's ICP

Companies or authorities may use the following non-exhaustive list of helpful questions pertaining to a company's ICP. The questions relate to all core elements, but not necessarily to every step described.

These questions can either be useful when developing an ICP, or at a later stage to review an existing ICP. They do not serve as a substitute for assessing your company's ICP against the details of the sections 'What is expected?' and 'What are the steps involved?' in the main part of this guidance. The answers to these questions should also not be understood as a reassurance of a proper ICP for dual-use trade control.

1. **Top-level management commitment to compliance**

— Is a top-level management commitment clearly stating the company's commitment to dual-use trade controls available?

— Is the statement easily accessible for all employees?

2. **Organisational structure, responsibilities and resources**

— Did your company nominate the person(s) in charge of answering employees' questions on the company's compliance procedures, on a suspicious enquiry or on possible violations? Are the contact details of the responsible person(s) available to all affected staff?

— What are the parts or activities of your company that are concerned by dual-use trade control and compliance?

— In which part of your company is the dual-use trade compliance personnel situated? Could there be a conflict of interests?

— In case your company decides to outsource the dual-use trade compliance management, how is the interaction with your company organised?

— How many people are either employed solely to deal with dual-use trade control or have responsibility for it with other tasks? Are back-up persons available?

— How is the relationship between the export control staff and the top-level management organised, for example, concerning information exchange?

— Does your company document and distribute the set of policies and procedures addressing dual-use trade controls to all relevant personnel? In what format?

— Are there electronic tools available that assist your company's compliance procedures?

3. **Training and awareness raising**

— Does your company provide for (tailored) compliance training or awareness raising activities?

— What compliance training or awareness raising formats does the company offer? Examples are: external seminars, subscription to information sessions offered by competent authorities, in-house training events, etc.

— How is it ensured that dual-use trade control staff have access to all relevant laws and regulations?

4. **Transaction screening process and procedures**

4.1. *Item classification*

— Are all export relevant products assessed against the EU and national dual-use control lists or restrictive measures, and who is responsible for this?

— Is your company involved in the electronic transmission of dual-use software or technology? If so, how does the company ensure compliance with the electronic transmission of software or technology?

— Are there procedures in place for employees accessing controlled technology or software when visiting abroad?

— Is the classification of products received or manufactured by the company recorded?

— Are changes in the national and EU dual-use control lists translated into the company's classification procedures?

— When considering Article 22(10) of the EC dual-use Regulation (EC) No 428/2009, do the commercial documents relating to intra-EU-transfers of listed dual-use items listed mention that those items are subject to controls if exported from the EU?

4.2. *Transaction risk assessment*

See Annex 2 for a non-exhaustive list of 'red flag' questions that can support your company's transaction screening process to detect suspicious enquiries from customers.

— What are the procedures for dealing with positive and negative results from the transaction risk assessment?

— How are 'false positive' results (i.e. an unnecessary hit of concern) from the transaction risk assessment resolved?

Checks on embargoed, sanctioned or sensitive destinations and entities

— During the transaction risk assessment, how does your company take into account restrictive measures (including sanctions)?

Stated end-use and involved parties screening

— What are the internal procedures for the stated end-use and involved parties screening process?

— How are (new) involved parties screened? Do you periodically screen existing customers again?

'Catch-all' controls for non-listed dual-use items

— How is information of concern about the stated end-use (in the sense of the catch-all provisions ([1])) collected and put to use?

Diversion risk screening

— Has your company procedures in place for risk diversion screening?

4.3. *License determination and application, including for controlled brokering, transfer and transit activities*

— How is it ensured, that in each individual case the correct license type (individual, global or Union general licenses) is applied for/used?

— How is it ensured, that less obvious types of exports and other activities that are subject to restrictions are recognised as such and do not take place contrary to EU and Member State dual-use trade control laws?

4.4. *Post-licencing, including shipment control and compliance with the conditions of the authorisation*

— Does a final transaction risk assessment take place before the shipment?

— How does your company ensure that the terms and conditions (including reporting) of the licence(s) are being complied with?

5. **Performance reviews, audits, internal reporting and corrective actions**

— Are the daily relevant business operating procedures subject to a (random) dual-use trade control performance review?

— Does your company have internal or external audit procedures in place?

— Does your company have whistleblowing or escalation procedures in place?

— What corrective actions does your company undertake in case of non-compliance?

([1]) Article 4 of Regulation (EC) No 428/2009.

6. **Recordkeeping and documentation**

— What are the company's procedures for filing and retrieving documents related to dual-use trade control? Did your company consider including a record of past contacts with the competent authority?

— Are the legal requirements for recordkeeping known to the dual-use trade control staff and relevant commercial partners?

— Are records being inspected for completeness, accuracy and quality?

7. **Physical and information security**

— Does your company implement cybersecurity measures to protect dual-use software and technology and ensure that they do not get lost, are easily stolen or exported without a valid license?

— Can your company identify critical steps and related physical and information security vulnerabilities regarding dual-use items?

Annex 2

'Red flags' relating to suspicious enquiries

Being vigilant for signs of suspicious enquiries or orders is vital for countering the risks of the proliferation of Weapons of Mass Destruction, their means of delivery, and the destabilising accumulations of conventional weapons. Sharing such information with your competent authority is highly recommended and in some cases may be mandatory under EU and national laws and regulations. In case of doubt, consult with the competent authority.

The below non-exhaustive list of 'red flags' is based on existing best practice and is derived from:

— the Wassenaar Arrangement list of advisory questions for industry (Agreed at the 2003 Plenary and review agreed at the 2018 Plenary)

— the 2010 Compliance Code of Practice (Department for Business Innovation & Skills, United Kingdom) and

— ICP approaches from competent authorities in other EU Members States.

Based on your company's experience, additions or amendments to the list below can be made. You know best what is suspicious within your business area.

Your company should be vigilant if one or more of the following 'red flags' are detected:

Your product(s)

— your product is still being developed or has not yet found many customers in your domestic market;

— the characteristics of your product are technically superior to those of established competitors;

— your customer requested unusual customisation of a standard product, or modification requests raise concerns about potential applications of the customised product;

— your product has known dual-use, military, or sensitive application;

End use and End user

— the customer is new to your company and your knowledge about him/her is incomplete or inconsistent or it is difficult to find information about the customer in open sources;

— the stated end user is a trading company, distributor or based in a free trade zone so that your company might be unaware where your product(s) finally ends up;

— the end user is tied to the military, the defence industry or a governmental research body and the stated end use is civilian;

— the customer seems not to be familiar with the product and its performance characteristics (e.g. an obvious lack of technical knowledge);

— the customer requests a product that seems overly capable for the intended application;

— the contact information in enquiries (e.g. phone numbers, email and addresses) is located in other countries than the stated company, or changed to that over time;

— the company has a foreign company name (e.g. in a language that is unexpected for the country where headquarter is located);

— the company website lack content in comparison to what is normally found on a legitimate company website;

— the customer is reluctant to offer information about the end use of the items (e.g. via an end-user statement), provide clear answers to commercial or technical questions which are routine in normal negotiations or to provide an end user statement;

— an unconvincing explanation is given as to why the items are required, given the customer's normal business, or the technical sophistication of the items;

Shipment

— unusual shipping, packaging or labelling arrangements are requested; usual incoterms for shipment, the sealing of containers/trucks and the confirmation of receipt by the consignee/end-user are refused;

Finance and contract conditions

— unusually favourable payment terms such as paying an unreasonable high price, full payment in advance or want to do a full cash payment immediately;

— the payment is made by other parties than the customer or stated intermediaries and follow another route than the products;

— routine installation, training or maintenance services are declined;

— the installation site is in an area under strict security control or is in an area to which access is severely restricted,

— the installation site is unusual in view of the exporter's line of business or is unusual in view of the type of equipment being installed;

— there are unusual requirements for excessive confidentiality about final destinations, or customers, or specifications of items;

— there are requests for excessive spare parts or lack of interest in any spare parts;

Sharing information about suspicious enquiries with your competent authority is highly recommended and a good business practice. Additionally, where appropriate, information-sharing within the companies' supply chain and with other exporters may be valuable in light of the risk that proliferators send requests to different companies, hoping that one of the requests may be successful or with the aim of acquiring a critical amount of material from different sources (where each individual request would not yet raise suspicion). In case of doubt, consult with the competent authority.

Annex 3

List of EU MS competent export control authorities

http://trade.ec.europa.eu/doclib/docs/2016/august/tradoc_154880.pdf