European Commission

JRC SCIENTIFIC AND POLICY REPORTS

Strengthening Strategic Export Controls by Internal Compliance Programmes.

Second Revision

2014

Joint Research Centre

Europe Direct is a service to help you find answers to your questions about the European Union
Freephone number (*): 00 800 6 7 8 9 10 11
(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server http://europa.eu/.

Printed in Italy

Contents

Table of Contents

Acknowledgements

Introduction

Strategic export control[1] is one of the pillars of nuclear non-proliferation, and complements both the international safeguards and physical protection regimes. It monitors and controls international transfers of nuclear and non-nuclear materials, technology and equipment. Since the end of WWII, the State-level proliferation in the 60's and 70's, and the advent of transnational illicit procurement networks in the 90's and early 2000s, the awareness of WMD proliferation risks has grown.

Non-proliferation measures no longer focus solely on the State but has been broadened to a trans- (and sub-) national dimension, addressing proliferation networks, terrorists and other non-state actors.

These challenging circumstances triggered the development of the export control regimes (Zangger Committee, Nuclear Suppliers Group, Australia Group, Missile Technology Control Regime and Wassenaar Arrangement), EU regulations and national laws. There is an increasing acknowledgement that exporters also have an important role to play in ensuring compliance with export controls. Without access to supplies from high-tech companies and technology holders in particular, the development of WMD and delivery means by countries of concern and proliferation networks would be much harder, if not impossible. Exporters are therefore the first line of defence against illicit procurement attempts.

The reform of the EU legal framework in 2009 (Regulation (EC) 428/2009, hereinafter called DU regulation) placed an increased emphasis on the responsibility of the exporter. For instance, the catch-all provision in article 4 of the DU Regulation not only require a licence for non-listed items if the exporter has been informed by his national authority, but also if the exporter is aware or has grounds for suspecting that the items will be used for WMD proliferation purposes.

Despite the Single Market, the DU regulation still includes an authorisation process for intra-EU transfers of a range of sensitive items. Brokering and transit are included to fulfil obligations placed on States by United Nations Security Council Resolution (UNSCR) 1540. The Regulation also addresses *Intangible Technology Transfers* (ITT), an increasing proliferation vulnerability (through e-mails, training, invited talks and the latest development, cloud computing). ITT constitutes a major challenge to enforcement of controls as it effects not only industry but research organisations and universities when working across geographic boarders.

A careful examination of the provisions of the DU regulation reveals that there is no concrete obligation on industry and research centres to develop Internal Compliance Programmes or other compliance mechanisms. The only compliance mechanism is set out in article 20 and concerns a requirement for exporters and brokers of dual-use items to keep detailed registers or records of their exports, in accordance with their respective national law or practice.

Contrary to the DU regulation, the Council's "New Lines for Action in combating the proliferation of WMD and their deliveries" provides for the adoption of awareness raising models for undertakings, scientific/academic circles and financial institutions[2].

The international export control regimes are based on politically binding, as opposed to legally binding, agreements. Only the Wassenaar Arrangement has done any work on codifying ICPs. UNSCR 1540, which is legally-binding on States, calls on them to implement an efficient export control systems to prevent illicit trafficking. In this respect it is clear that only States whose exporters comply with the DU export control regulatory framework can contribute to such a challenging effort. Those who do not comply - out of lack of information, negligence, or malevolent attitude – greatly reduce its efficiency.

---

[1] By export control we mean the control of exports, transfer, brokering and transit of dual-use items. By exporter we mean the one who is doing one of these activities. For the fluency of the paper, we choose to use "export control" and "exporter" as collective nouns.

[2] Council of EU - General Secretariat, *New Lines for Action by the European Union in Combating the proliferation of WMD and their Delivery systems,* 17172/08, Brussels 17 Dec. 2008. Retrieved from: http://trade.ec.europa.eu/doclib/docs/2008/december/tradoc_141740.pdf

Awareness and compliance, triggering the export authorisation process in circumstances where this is required, are the primary elements of an effective export control system. The system cannot be effective if it relies solely on enforcement action, fines and imprisonment.

Internal Compliance Programmes

Internal Compliance Programs (ICPs) promote awareness raising and the fulfilment of export control requirements by exporters (e.g. the supply chain, systems integrators, distributors and others such as research centres).

They can also enhance communication and cooperation between the State and the exporter (ISIS, 2003:2). In France, for example, the ICP is the first personal link between the authorities and industry (Paile, 2011:70). The ICP assists the exporter to manage the exports of dual-use goods and technologies and to meet the export control requirements of their national system.

A properly implemented ICP provides an organisation exporting sensitive items and technologies with a structured approach, and supports a culture of doing business in ways that ensure delivery of items to legitimate end-users thus minimizing the risk of diversion.

ICPs require an exporter to introduce clear policies and procedures that will be easily understood by staff, thus reducing the likelihood of mistakes. The shipment of any dual-use equipment without due authorisation, even if this is to a non-sensitive customer, may have adverse consequences for both international security and the exporter's business and its employees (e.g. contribution to illicit procurement and proliferating activities of end-users; withdrawal of a company's exporting privileges; other administrative penalties, fines and imprisonment).

According to the Guidelines of the Wassenaar Arrangement (2011:1) an ICP is not legally binding but recommended. It is the duty of the State to encourage, where appropriate, its exporters to develop and implement ICPs. It may assist by providing expertise and guidance material on ICPs in any relevant form, including seminars and the opportunity to audit the draft ICP. The State may also consider measures and stimuli in domestic laws and regulations encouraging exporters to introduce an ICP. ISIS (2003) points the government's role in developing policies to better regulate export controls and create an environment supportive of non-proliferation efforts. The implementation of an ICP is the responsibility of both the State and the exporter.

There is no consensus amongst EU Member States on the need to impose an ICP obligation on exporters. According to art.12.2 of the DU Regulation the national authority, when assessing an application for a global authorisation, shall take into consideration the compliance of the exporter with the provisions and objectives of this Regulation and with the terms and conditions of the authorisation. Some Member States (Finland and Romania) interpret art.12.2 as requiring an exporter to have an ICP in place before they will issue a global authorisation (Article 23 Coordination Group, 2011: question 1). Other Member States (Estonia, Poland and UK) challenge this interpretation. According to these Member States, the fact that the exporter must have proportionate and adequate means to ensure compliance with the DU Regulation does not require implementation of a formalised ICP.

COMMISSION RECOMMENDATION (2011/24/EU) of 11 January 2011 on the certification of defence undertakings under the EU Directive on intra-community transfer of defence related products contains criteria for assessing whether a company qualifies for certification. These criteria are essentially guiding governments on evaluation of ICPs or their equivalents.

In some countries outside the EU implementation of an ICP is viewed as proof that an exporter takes his export compliance responsibilities seriously. For example in Japan, the Ministry of Economy, Trade and Industry (METI) publishes on its website the names of those companies that have registered their ICPs and agreed for this information to be made public (METI, 2007). Companies do this because they see it as a way of demonstrating to the public that they are a company of good standing.
These various interpretations show that a further analysis would be useful.

Types of exporters

Is the exporter a manufacturer or an academic institute? Does it perform commercial activities or research? Exporters can be:-

- Nuclear operators
- *Nuclear technology holders*
- Design and consulting services
- Manufacturers of dual-use goods
- research centres
- universities,
- system integrators
- suppliers
- distributors
- brokers
- governmental and international organisations, e.g. for cooperation and assistance

Issues

The type of business/activity and organisation/geographic location will determine the nature of the compliance programme to be implemented.

For instance, a company with subsidiaries in 3rd countries will have to comply with the export control laws and regulations of every country where they operate. This may include ensuring that the re-export restrictions placed on an item by one country are adhered to when it is exported from another. It may also involve imports and exports associated with internal processing with its branches located abroad. This applies equally to the transfer of technology, as well as parts and components, and possibly may require authorisation for movements between EU Member States.[3]

Industry and research organisations will find themselves needing to consider whether their work is subject to intangible technology transfer controls (ITT) if they are co-operating with anyone in a 3rd country (***ref. EXP-WG presentations***).

Exporters of goods and services will also need to ensure that they comply with technical assistance controls when providing such a service.

In conducting their research, scientists often need to exchange information and results with colleagues all over the world. International joint projects may also deal with controlled technology and multi-national regulatory frameworks. In this context, it is not always clear when information can be considered part of the "public domain" or is considered to be "basic scientific research" both of which are not controlled. The Horizon 2020 Human Security Research Toolkit will provide guidance to project proposers.

No one size fits all approach

Each exporter has to tailor its ICP to its own characteristics (e.g. size, nature of items exported, national, regional or global footprint).

Several ICP models, guidelines and examples are available from open sources. However, they have to be tailored to the organisation. There is no one size fits all approach.

Small companies may not need an Export Control Unit or an export control officer in each business unit (as can be the case in larger companies). The export control responsibility may be able to be managed by one person,

---

[3] Intra-EU transfers apply to items include in Annex IV of EU dual-use regulation

possibly along with other tasks. In universities and research centres, an Export Control Unit would not be necessary if the number of controlled exports was limited. Such companies and institutions would probably also lack the resources to afford to pay for an external audit. In such cases the task could fall to the person in charge of export controls. National authorities may provide assistance and guidance on ICPs and audits that may be of help.

Some states[4] expect a more developed ICP in large organisations with extensive exports (Article 23 Coordination Group, 2011: question 3). Beside the size, the volume of controlled items transacted is relevant. A large organisation with very few controlled exports will need to devote less time and resources to implementing an ICP than a small or medium size organisation where all items appear on the control list.

It is widely recognised that establishing an ICP carries costs (SEESAC 2011:8). An organisation will need to allocate resources (time, financial and human). However an effective compliance programme offers many advantages. Efficient implementation of export control compliance will ensure that they are not an impediment to business. Compliance can be used as a positive differentiator in bids and a compliant company will be able to respond to customers faster because they understand the export control regime they are working in. Regulators may grant compliant companies' access to licences not available to competitors if they have an ICP. Compliance will help business avoid negative and damaging publicity, costly fines and prison for employees and senior management.

Once an ICP has been introduced, work is not finished. An ICP is a living document. It needs to be updated to take account of changes in national laws and regulations, to changes in organisation, structure and business model and reviewed regularly after audits.

The end-use and sensitivity of items is key to deciding whether an ICP is needed. Even if no goods, software or technology appear on the control list export controls may still apply if the exporter is aware, has been informed by government or has grounds to suspect that they may contribute to proliferation activities.

The U.S. Department of Commerce (2011:3) provides in its guidelines a list of variables that influence an ICP:

   a) Size of the organisation;
   b) End-use and sensitivity of products;
   c) Geographic location of business and customers;
   d) Relationship with business partners;
   e) Volume of exports;
   f) Products restrictions;
   g) Complexity of internal export processes.

Looking at these variables it is useful to draft a risk-profile of the organisation, identifying ICP issues, as e.g. indicated by The Metropolitan Corporate Counsel (2007):

   a) Identify relevant business activities;
   b) Examine potential risk areas in its client base;
   c) Identify products or services that the company offers that may attract sanctioned countries;
   d) Examine its marketing practices;
   e) Assess the risk-sensitivity of the company.

ICP Basic Elements

A comprehensive analysis of the key elements of an ICP is a preliminary step to understanding how to implement an ICP. Though each organisation must undergo the same underlying analysis to identify risk areas, the actual elements of the final ICP will vary greatly from company to company. ICPs should contain a variant

---

[4]Ireland, Hungary, Sweden and UK.

of the elements listed below. Each organisation should determine which procedures to apply for each element to ensure the most effective and efficient ICP to suit its purposes (Rubinoff & Soliman, 2007). It is important that the ICP is an integrated programme. Each element of an ICP should build upon, and interconnect, with all other parts of the programme (U.S. Department of commerce, 2011:7).
See also "Leybold charter"

A general model of an ICP is set out below.

1. *Commitment to compliance*

The compliance statement, written by a senior representative, contains the exporter's awareness of and compliance with all domestic export control laws and regulations (and foreign laws and regulations where appropriate). The Senior Management's commitment to compliance underlines the importance of the ICP in the organisation and raises awareness within the company. It also establishes a culture of compliance. The commitment to compliance can also be referred in the corporate mission statement.
The "Compliance Code of Practice" of BIS (2010:13) gives an example of the commitment to compliance issued by senior management (see Annex 1).

Key elements of the Commitment to compliance
Senior representative

2. *Written Export Management & Compliance Programme*

An ICP requires the development of an Export Management & Compliance Programme to communicate management commitment to the ICP and to outline the basic guiding principles. A written Export Management & Compliance Programme is a tool for employees, a "map of compliance" to follow. It is important that it reaches all employees. Apart from employees directly concerned with the exporting process, others involved in such areas as design, development, engineering, research, purchasing, the supply chain, maintenance and after sales service must be made aware particularly as many of them will potentially be exporters of technology via email and other electronic means. It is also critical to ensure that the IT department's strategy takes account of and is fully compliant with intangible technology controls.

The programme should include a statement of commitment to compliance written by a senior representative, the basis of the compliance training programme, the compliance policies and step-by-step procedures, the point-of-contact (the person responsible for export control) and the disciplinary measures in case of violation of the export control laws and regulations. It should be as short and simple as possible, illustrated with visual aids (matrices, flowcharts and checklist) (M.E. Dey & Co, s.d.).

Key elements of the written Export Management and Compliance Program
Written statement by senior representative
Training program
Compliance policies
Step-by-step procedures
Point-of-contact
Disciplinary measures in case of violations

3. *Responsibility*

The organisation needs to appoint a person responsible for overall compliance with export controls. The person charged with this responsibility needs to be a senior representative (director or other individual of corresponding status) because he has to carry personal responsibility for export control compliance within the

organisation. Below that person an export control manager (and deputies where the size of the organisation requires it) would be tasked with day to day operation of the compliance regime within the organisation. That person should not be part of the sales department or any other export oriented unit to avoid conflicts of interest. His source of salary and evaluations should be separated from the businesses that he monitors (U.S. Department of Commerce, Bureau of Industry and Security, 2011:49). That person would be responsible for applying for export authorisations and would also need the authority to stop a delivery if there were doubts about its compliance with export controls. He acts as the internal (for his colleagues) and external (towards the national administration) first point of contact. A backup[5] would be required to cover for absences and any gaps should the export control manager leave to join another organisation or retire.

Based on the Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies agreed by the Wassenaar Arrangement at the 2011 Plenary the export control manager would be responsible for:

f)   Development and update of the ICP;
g)   Development and revision of operational procedures;
h)   Staying-up-to-date with changes to relevant regulations and with any directions or guidance issued by the competent authorities;
i)   Classification/identification, screening and approval of business transactions;
j)   General export control management, throughout the business, including direction and communication;
k)   Assignment of personnel in charge of auditing;
l)   Training.

Another duty sometimes assigned involves the development of procedures for cooperating with the state's administration, as is required by the Polish government (Ministry of Foreign Affairs of Poland, s.d.).

Key elements of responsibility
Independent
Bear the appropriate responsibility
Define the duties

4. Export screening procedures

Export screening procedures are the core of an ICP. There are a number of checks that need to be made as described below. Screening should take place when an order is received and prior to shipping the product in the event there has been a change to the control lists during the processing time (U.S. Department of Commerce, Bureau of Industry and Security, 2011:93). A similar screening of all parties to the contract also needs to take place to ensure that they have not been placed on a denied parties list.

a) Classification/identification procedure

This step is at the very heart of the process. It is necessary to determine whether items to be supplied are subject to any restrictions on their export. The properties of the items must be evaluated against the relevant control list to determine whether an authorization is required. In most organizations those responsible for the technology (e.g. engineering) would be responsible for undertaking the classification exercise which would be validated by the export control manager. Where necessary, competent authorities should be consulted to agree a product rating. A record of all ratings for products, parts and components, software and technology should be kept to prevent needless repetition every time an order is received for the same item. However the record needs to be regularly reviewed to ensure that it takes into account changes to control list entries as these lists are subject to change.

---

[5] There should be at least two people able to carry this responsibility in case of holidays, illness etc.

Product classification can be time consuming and expensive depending on the product portfolio and number of items that need to be rated.

The exporter needs to cross check their products against the control lists contained in applicable national laws, e.g. for the "EU dual-use control list" (Annex I to the DU Regulation, recently amended as Regulation 388/2012), used also in other countries, possible additional national lists; other applicable lists in non-EU countries; sanctions control lists (e.g. targeting Iran, DPRK); EU Common Military List; other regulations e.g. the EU anti-torture regulation. Another mandatory step required In parallel[6] is to attribute a Harmonised System code needed to define the appropriate customs duties (quoted from discussions at "Global Trade Compliance and Export Control for the Oil & Gas Industry", London, 2013).

The difficulty of the task is recognised by some States. In the Request for a Comprehensive Review of Japan's Security Export Control Legal System (2010:17), it is proposed that the government supports the classification process by providing necessary services to exporters[7].

b) End-use screening

The purpose of the transaction and the plausibility of the end-use stated by the client needs to be evaluated. The annex to the "Statement of Understanding on Implementation of End-Use Controls for Dual-Use Items" agreed by the Wassenaar Arrangement (2007) provides basic and additional elements that can be applied. The establishment of an ICP is regarded as a basic element. End-use needs to be considered in the run-up to the submission of an export licence application. The exporter needs to present a factually complete licence application, including all necessary supporting documentation.

c) Customer/end-user screening

The exporter needs to asses if the customer is the end user, and if the activities of the customer/end-user are relevant to the exported item.

The exporter also needs to ascertain whether the destination of the item and all parties to the transaction are subject to any restrictions. In this respect, the U.S. Bureau of Industry and Security has developed a "Denied Persons List". This list helps companies to recognize potential violators of export laws and other parties who are known to have previously engaged in illicit procurement behaviour. This list is posted on their website (U.S. Department of Commerce, 2011:9). Other countries refer to the UNSCR database containing lists of names of individuals and companies who are known to be associated with illicit procurement efforts, which are widely available. The EU includes lists of entities and individuals in Regulations containing measures targeting certain countries (e.g. Iran, DPRK) or terrorist activities.

The Wassenaar Arrangement (2003) published a non-exhaustive list of questions ("red flags") guiding companies when suspicion should be raised and contact with national export licensing authorities might be advisable (see Annex 2).

d) Checking for catch-all requirements

For items that do not appear on a control list this stage allows checking to see whether the competent authorities may require a license for the export of a non-listed item. Non-listed items may be subject to a 'catch-all' if the exporter is aware, informed or has ground to suspect that they may contribute to a proliferating activity.
The qualifying cases invoking such a requirement are: items with potential WMD end-uses; items with a possible military end-use if exported to an embargoed destination; items which are intended to be used as parts or components of listed military items that have been exported without authorisation. When any question arises, the competent national authority should be consulted.

---

[6] A Correlation table between Dual Use and Combined Nomenclature codes is available on TARIC's web-site managed by DG TAXUD

[7] For this reason, Japan industries have set up CISTEC

All transaction screening procedures help to prevent the diversion of the export/transfer to an unauthorised end-user or end-uses.

AREVA (2012) formulates several guiding questions for the screening procedure:
- What is my item?
- Where is it going?
- Who will receive it (consignee)?
- Who will be the end user
- What will be the end-use?
- What else does the end-user do?

General Electric (2012:5) defines the same questions as the four W's of export control compliance (What, Where, Who and Why).

Key elements of screening procedures
Classification/identification procedure
End-use screening
Customer/end-user screening
Information by the competent authorities

5. Shipment control

Before shipment, the classification/identification and transaction screening procedures must be completed. This stage verifies that those tasks have been completed. It is also there to ensure that the declaration on export instruction documents and/or export licences for the goods and/or technology is correct and that quantities to be exported are permitted by the license.

Key elements of Shipment Control
Confirmation of the classification/identification and transaction screenings
Confirmation of the declarations

6. Performance review or compliance check

As already mentioned an ICP is not a static document and should be reviewed regularly. To do this, the exporter will need to establish a performance review process. This review will examine whether the export control operation has been implemented in accordance with the policies, processes and procedures set out in the ICP and that these are in conformance with all relevant laws and regulations. This review should be carried out annually. It can be performed internally or by an external body.

Appropriate key performance indicators should be developed to establish the robustness of the export control system.

Key elements of Performance review
Export control in compliance with the ICP and its operational procedures
Export control in compliance with all relevant laws and regulations
Annually

BIS (2010:29) provides in annex 6 of its Compliance Code of Practice a checklist for audits of internal compliance procedures. A list is also reported in the intra-EU arms directive (Annex 5).

7. Training

Staff training is important to maintain a successful ICP. Apart from employees directly concerned with the exporting process, others involved in such areas as design, development, engineering, purchasing, the supply chain, provision of IT, maintenance and after sales service must be trained.

This includes personnel who can export technology via electronic means (ITT) and those involved in arranging the movement of goods to third countries (BIS, 2010:9). They all need to be made aware of relevant export control laws, regulations, policies, control lists and amendments as soon as they have been published. According to ISIS (2003:10), employees should not only learn about specific export regulations they should be made aware of the capabilities of the products the company exports, ways in which such products can be misused, and how to identify illicit procurement attempts.

Before training is provided, the exporter needs to assess the current training programme and training needs. Based on these results a training plan can be developed (U.S. Department of Commerce, 2011:36). Participation in external events should be encouraged and special training should be provided for new employees. It is recommended that companies should investigate what assistance the national authority provides on this subject. For example, the Polish government provides an annual training fund for companies to use (SEESAC, 2011:29).

As part of the ICP process it is important to document attendance at training programmes and courses completed.

Key elements of Training
Continuous training
External training
Training for newcomers

8. Record keeping

National export control regulations require that records of exports and related documentation are retained for a specified period. According to Guidelines from the Wassenaar Arrangement (2011:7) these documents may include export licences, end-use statements, end user certificates, commercial invoices, clearance documents, product classification/identification sheets and records of electronic transfers.

The exporter should establish a policy on the time, mode and place for maintaining and storing records so that they can be easily retrieved (BIS, 2010:11).

Key elements of Record keeping
National legislation

9. Reporting and corrective action

An ICP needs to include policies and procedures on reporting and corrective action when a violation of export controls has been identified. When a violation, or suspected violation, of export control regulations or ICP procedures occurs, a prompt report should be made to the person responsible for export controls. Confirmed violations of regulations should be reported without delay to the competent authority as a v**oluntary disclosure**.

An ICP should encourage employees to report violations without the fear of consequence.

Procurement requests turned down because of suspicions that they are illicit attempts to gain products or technology should be reported to the relevant authorities. For nuclear related cases the IAEAs Procurement Outreach Programme collects such information from contributing States.

In exceptional circumstances where a member, or members, of staff have colluded to deliberately circumvent export controls disciplinary procedures should be implemented.

Where infringements were caused by human error or a lack of awareness follow-up would form part of any corrective action deemed necessary. Any corrective action should be implemented to ensure similar violations will be avoided. (Guidelines of the Wassenaar Arrangement, 2011:7).

Key elements of Reporting and Corrective Actions
Report to the responsible person
Report to the competent authority
Disciplinary procedure
Corrective action

10. Communication

At all times, and in ways defined by each organisation, proper and timely communication is a crucial element for a successful and efficient ICP.

Conclusions

The basic or key elements of an ICP were discussed in this essay. Introducing an ICP in an organisation can mean big changes (to working methods, to responsibilities and for teams). Often change will meet with resistance.

A transparent and persuasive communication can temper this resistance. For an ICP to be successful it needs the support of the whole organisation and become embedded in its culture.

Maintaining an ICP is a challenge further complicated by evolving regulations, globalisation, geopolitical issues and trade patterns.

A follow up to this note will attempt to address specific exporters, such as those involved in research, as well as ITT and related threats to the control of technology transfer. These merit specific attention because of the possible consequences of unintended transfer without proper authorisation. This document will examine the issues and remedial measures that need to be implemented to preserve legitimate trade and exchange of information.

Bibliography

- AREVA, (2012). *AREVA ICP,* presentation ESARDA Export Control Working Group, 23p.
- ARTICLE 23 COORDINATION GROUP, (2011). *Analysis of responses to the questionnaire on Internal Compliance Programmes and Article 12(2),* European Commission, official use only
- BIS (Department for Business, Innovation and Skills, Export Control Organisation), (2010). *'Compliance Code of Practice'*, 36p, on http://www.bis.gov.uk/assets/biscore/eco/docs/compliance-code-practice.pdf (last consultation on 01/03/2012)
- BRYAN CAVE Consulting, (s.d.). *Emerging Export Control Regimes in ASEAN & Best Practices for ICP: Challenges and Pitfalls,* 42p
- ISIS, (2003). *Key Elements of an Effective Export Control System*, on http://www.exportcontrols.org/print/key_elements.htm. (last consultation 21/03/2012).
- GENERAL ELECTRIC, (2012). *'Export Control Compliance at General Electric',* presentation by K. J. Cuddy, 13th International Export Control Conference, 7p.
- M.E. Dey & Co, (s.d.). *Export and Import Compliance Programs,* 12p., on http://medey.com/pdf/Export%20and%20Import%20Compliance%20Programs.pdf (last consultation 22/03/2012).
- Ministry of Economy, Trade and Industry of Japan, (2007). *Internal Compliance Program (ICP),* 14p., on http://www.meti.go.jp/policy/anpo/englishpage/icp.pdf last consultation 21/03/2012).
- MINISTRY OF FOREIGN AFFAIRS of Poland – Security Policy Department. (s.d.). *Internal Compliance Program – why and how?*, presentation, 11th International Export Control Conference, 25p., on http://exportcontrol.org/library/conferences/2706/38_Day_2-Industry-Ses_III-Pres_3-Firkowski.pdf (last consultation 07/03/2012).
- PAILE, S. (2011). *France. From Security to Competitive Security*, In MICHEL, Q. (ed.) (2011). Sensitive Trade. The perspective of European States, Brussels: P.I.E. Peter Lang, pp.61&74.
- Rubinoff, E. L. & Soliman, T. A., (2007). *Developing And Implementing An Internal Compliance Program To Address Economic Sanctions Concerns*, In The Metropolitan Corporate Counsel, 1 April 2007, p23., on http://www.metrocorpcounsel.com/articles/8135/developing-and-implementing-internal-compliance-program-address-economic-sanctions-con (last consultation 22/03/2012).
- SEESAC, (2011). *Internal Compliance Programs*, 54p., on http://www.sipri.org/research/armaments/transfers/publications/other_publ/other%20publications/Internal%20Compliance%20Programmes.pdf (last consultation 22/03/2012).
- U.S. Department of Commerce, Bureau of Industry and Security, Office of Exporter Services, Export Management and Compliance Division (2011) *Compliance Guidelines: How to develop an effective export management and compliance program and manual*, 166p., on http://www.bis.doc.gov/complianceandenforcement/emcp_guidelines.pdf (last consultation 22/03/2012).
- US DOE NNSA, (2012). *Assessing Proliferation Risk: End-Use/End-User Analysis,* presentation at the Seminar on Export Control technical issues, 27p.
- WASSENAAR ARRANGEMENT, (2011). *Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies*, 7p., on http://www.wassenaar.org/guidelines/docs/2%20-%20Internal%20Compliance%20Programmes.pdf (last consultation on 01/03/2012).
- WASSENAAR ARRANGEMENT, (2007). *Statement of Understanding on Implementation of End-Use Controls for Dual-Use Items,* pp.73-77, in WASSENAAR ARRANGEMENT, (2012). *Basic Documents. Compilation,* 130p.
- Nuclear Suppliers Group web-site: Good practices for corporate standards
- COMMISSION RECOMMENDATION of 11 January 2011 on the certification of defence undertakings (Directive on intra-EU arms transfers)

Annexes

Annex 1: Example Commitment to Compliance

A MESSAGE FROM THE CHAIRMAN

"The success of this company depends in large part on the business we do overseas.

Export controls imposed by the UK Government and the European Community affect a high proportion of the products we see and many of our overseas markets. We must therefore understand the controls and be quite sure we comply with them. The purpose of these controls is to limit the supply of technology or strategic goods to countries proscribed, principally for reasons of proliferation, security, or terrorism. It is in the interest of us all that the controls are effective if it makes the world a safer place. For our business it is essential that we comply with the legislation: failure to do so would bring serious penalties for the company and for the individuals concerned.

I have nominated .... to be the person with overall responsibility within the company for export control matters assisted by …… and he/she will be reviewing the effectiveness of our current procedures in light of the Export Control Organisation's Code of Practice to which we shall adhere. But each of us must be aware of our own role and ensure that no items are despatched (remembering that this term also covers the transmission of software or technology by fax, telephone or other electronic media and arranging to move goods between third countries) without due clearance and authorisation. Information is available on how export controls affect your position; make sure you are aware of it."

Source: BIS, (2010). *'Compliance Code of Practice. Annex I'*, p .13.

Annex 2: Red Flags

The Wassenaar Arrangement (2003) published a non-exhaustive list of questions guiding companies when suspicion should be raised and contact with national export licensing authorities might be advisable.

1. Do you know your customer? If not, is it difficult to find information about him/her?
2. Is the customer or the end-user tied to the military or the defence industry?
3. Is the customer or the end-user tied to any military or governmental research body?
4. If you have done business with the customer before - is this a usual request for them to make? Does the product fit the business profile?
5. Does the customer seem familiar with the product and its performance characteristics or is there an obvious lack of technical knowledge?
6. Is the customer reluctant to provide an end-use statement or is the information insufficient compared to other negotiations?
7. Does the customer reject the customary installation, training or maintenance services provided?
8. Is unusual packaging and labelling required?
9. Is the shipping route unusual?
10. Does the customer order an excessive amount of spare parts or other items that are related to the product, but not to the stated end-use?
11. Is the customer offering unusually profitable payment terms, such as a much higher price?
12. Is the customer offering to pay in cash?

Annex 3: Checklist for internal compliance

Personnel
- *Are records of personnel involved in export control up to date?*
- *Have all employees who have the ability to make exports (remember that everyone with access to email, telephone and fax can potentially export technology) received the necessary induction or (re)training?*

Documents available
Do staff who need to have access to:
- *compliance procedures*
- *up to date legislation*
- *guidance notes/contact details?*

Product/licence
- *If there is a full product/country/licence matrix or similar, is it up to date?*
- *Was it checked against export control legislation and current company product range within the last three months? - if not a check/update should be arranged within the next two months.*
- *Are ratings of products up to date, including ratings in relation to new products or new markets?*
- *Have there been any changes to Open General Licences in the last few months, which means the goods/destinations, are no longer covered?*

Customer information
- *Is the necessary information reaching those responsible for licence processing, for example to ensure quick answers to end-use enquiries? - if not, should sales/marketing staff be reminded of what is needed?*
- *Should customers be alerted to the possible need for end-use information at an earlier stage (e.g. on quotation documents)?*
- *Is credit control information on customers' status being fed through for export control checks?*

Licence processing
- *Are licences held by the business up to date (for example, any changes in name or address duly notified)? Do the Open Individual Licences the company has have at least 6 months before they expire? If not has a new licence been applied for? If less than 3 months, has an extension been requested?*
- *Are end-use undertakings valid? Are they in the right format?*
- *Where individual licences are needed, is the procedure for applications working smoothly (and see Customer Information above)?*
- *If Open General Licences are used, has the business registered with ECO? Is the licence quoted correctly on the relevant documentation?*

Exporting goods
- *Are instructions to despatch department and/or freight forwarders up to date?*
- *Are they being adhered to (e.g. copies of export documentation returned within reasonable time)? - if not revise or restate the requirements and set a date to check on improvement.*

Record keeping
- *Selecting two or three cases at random, are the records (required to be kept under the licences) accessible?*
- *Are all related documents filed together or accessible through common fields?*

Resolution of problems
- *If aspects of procedures have been found unsatisfactory in the course of this check, or if problems have been encountered in operating the procedures, is there a plan for improvements?*
- *Have the necessary revisions or amendments been made known to the relevant personnel?*

Source: BIS, (2010). *'Compliance Code of Practice. Annex 6'*, p.29.

Annex 4: Flowchart ICP – Step by step

Define the organisation
- Be aware of the characteristics of the organisation (size, end-use and sensitivity of the products, geographic location of business and customers, relationship with business partners, volume of exports and controlled exports, products restrictions, complexity of internal export processes).
- Be aware of all the regulations the organisation has to comply with.

Develop the basic elements of the ICP
- The basic elements are written export management and compliance program, commitment to compliance, responsibility, export screening procedures, shipment control, compliance check, training, record keeping and reporting and corrective actions.
- The basic elements have to be developed according to the needs of the organisation. These are defined by its characteristics and the laws it has to comply with.

Review the current procedures
- Check the current implementation of business procedures that will be affected by the ICP (in accordance with the developed basic elements).
- Modify the business procedures to comply with the ICP (in accordance with the developed basic elements).

Establish missing procedures
- Draft missing procedures in cooperation with the units/persons concerned.

Implement the ICP
- Introduce the ICP by a company wide announcement (showing commitment of the management).
- Train relevant staff involved.
- Provide guidelines for the implementation.

Maintain the ICP up to date
- Update the product classification for each new product/technology.
- Stay up to date of the latest amendments on export control regulation.
- Provide training.
- Perform regular compliance checks (idealy annually).

Annex 5: Criteria referred to in Art. 9 of 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

Reliability shall be assessed according to the following criteria:

(a) *proven experience in defence activities, taking into account in particular the undertaking's record of compliance with export restrictions, any court decisions on this matter, any authorisation to produce or commercialise defence-related products and the employment of experienced management staff;*

(b) *relevant industrial activity in defence-related products within the Community, in particular capacity for system/sub-system integration;*

(c) *the appointment of a senior executive as the dedicated officer personally responsible for transfers and exports;*

(d) *a written commitment of the undertaking, signed by the senior executive referred to in point (c), that the undertaking will take all necessary steps to observe and enforce all specific conditions related to the end-use and export of any specific component or product received;*

(e) *a written commitment of the undertaking, signed by the senior executive referred to in point (c), to provide to the competent authorities, with due diligence, detailed information in response to requests and inquiries concerning the end-users or end-use of all products exported, transferred or received under a transfer licence from another Member State; and*

(f) *a description, countersigned by the senior executive referred to in point (c), of the internal compliance programme or transfer and export management system implemented in the undertaking. This description shall provide details of the organisational, human and technical resources allocated to the management of transfers and exports, the chain of responsibility within the undertaking, internal audit procedures, awareness-raising and staff training, physical and technical security arrangements, record-keeping and traceability of transfers and exports.*

Annex 6: Export Screening Procedures

WHAT?
Item

WHY?
End- use

WHO?
End-user

WHERE?
Destination
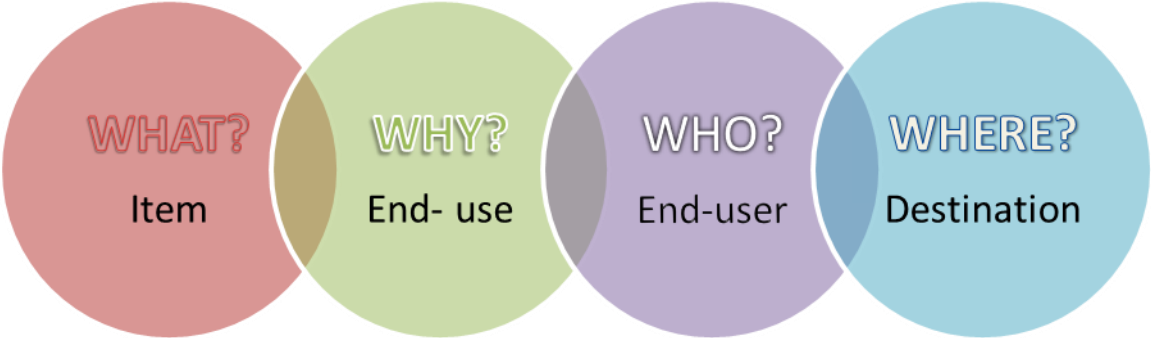
WHAT?
Item

Is an export licence required?
Are there proliferation concerns associated with this item?

Is the item appropriate for the stated end-use?

WHY?
End-use

Is there a possibility that the item being exported will be used in a military application or for chemical, nuclear or biological weapons proliferation?

Is the stated end-use consistent with the activities of the end-user?

WHO?
End-user

Has the exporter dealt with the end-user on many occasions in the past?
Is the end-user involved in any military or chemical, nuclear or biological weapons proliferation activities?
Has the end-user been screened? Have the existence and activities of the end-user been confirmed?
Is there anything about the transaction that raises a "red flag"?
Does the end-user appear on a denial list?

Can an end-use certificate been provided?
Is there a risk that the end-user will transfer the item to another person?

WHERE?
Destination

Are the final destination and transit/transhipment destination taken into account?
Is the destination of the export a country of concern? Is an export licence required?
Is the destination country a strategic ally or an adherent to a multilateral export control regime?
Is the destination of the export a country subject to unilateral or multilateral sanctions?
Does the destination country have its own export control laws and regulations?

Abstract

Awareness and compliance, triggering the export authorisations' process, are the primary elements of an effective export control system, which otherwise could not be based solely on enforcement at borders and prosecution.
ICP is a challenge further complicated by evolving regulations, globalisation, geopolitical issues and trade patterns.

A first note with overview of ICP issues and a general model, with a long list of references was published by JRC in 2013.

This second version has been commented and improved by the ESARDA Export Control Working Group in 2014.

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.