Part B: Complying with Trade Controls

6. Compliance: Designing Strategies - Adapting Policies - Developing Models

Ensuring compliance with the non-proliferation system is a crucial issue towards the attainment of non-proliferation objectives concerning essentially the enhancement of security and peace worldwide. Apparently, a first issue concerns the allegiance of States to the non-proliferation system as this is expressed with the signing and ratification of non-proliferation treaties and further undertakings assumed in the framework of bilateral agreements and politically binding arrangements. A second issue concerns whether States stick to the rules and enforce the requisite measures so that to achieve true compliance with the non-proliferation system in practice. The international system in general lacks an international governance and it is composed by States which may try to evade the rules and satisfy their own interests at the expense of non-proliferation objectives very much in the same way as individuals may violate or abrogate an agreement. For instance, non-compliance may be a deliberate effort of a State to pursue a covert nuclear weapons programme or to enable the transfers of dual-use items to proliferant States and/or outlaw organisations through funding or any other means. Non-compliance can be also a result of the weakness of a State to pursue the necessary measures guaranteeing the secure handling, storage and transfer of controlled material and equipment.

It follows that State commitments bring direct or indirect obligations for private actors and compliance measures seek to eliminate the possibility for infringements perpetrated by both State and non-State actors. This chapter emphasizes what non-State actors could do in order to meet their ever increasing responsibilities as laid down in the dual-use export control laws and in line with the expectations of society. Given that firms and public research organisations operate in an environment entrenched by rules and obligations set by governments the role of the latter in stimulating, encouraging and promoting compliance and self-regulation efforts is crucial.

6.1 Complying through the implementation of Internal Compliance Programmes

The elusive nature of export controls lies partly in the far-reaching impact of the provisions and partly in the inherently dual nature of the controlled items. Export control provisions may demand the assumption of a more proactive and responsible role from the side of non-State stakeholders. Although this is not always explicitly demonstrated or sufficiently elaborate in the export control legislation, the engagement of exporters and their collaboration with the government is an important prerequisite for the effective implementation of trade control laws. Exporters including research and academia should be encouraged to embed the concept of compliance not just in their procedural arrangements but also in their own mind-sets[326]. In the EU, Article 4 §4 of the Regulation requires from

[326] F. Sevini et al. "Nuclear Suppliers' Enhanced Export Control Compliance and Communication with Authorities," Proceedings of 37th ESARDA Annual Meeting, Publications Office of the

exporters to notify the competent authorities in the case where they are aware that a non-listed item they intend to export will be used for the development of WMD or other military uses as specified in paragraphs 1 to 3 of the same article (catch-all clause). Moreover, Article 4 §5, known also as 'the suspicion clause' provides that a Member State may adopt or maintain legislation allowing the imposition of an authorisation requirement if there is a -logically convincing- suspicion by the exporter that a non-listed item would be used for WMD purposes.

> If an exporter is aware that dual-use items which he proposes to export, not listed in Annex I, are intended, in their entirety or in part, for any of the uses referred to in paragraphs 1, 2 and 3, he must notify the authorities referred to in paragraph 1, which will decide whether or not it is expedient to make the export concerned subject to authorisation.
>
> A Member State may adopt or maintain national legislation imposing an authorisation requirement on the export of dual-use items not listed in Annex I if the exporter has grounds for suspecting that those items are or may be intended, in their entirety or in part, for any of the uses referred to in paragraph 1.
>
> *Article 4 §4 and §5 of the regulation 428/2009*

These provisions may seem well-anticipated or even common sense. If one knows that the item he produces will be used in connection with an illegal weapons program he will be expected to notify the competent authorities about such a contingency and not proceed further with the export of the item in question. Codifying such patterns of responsible behaviour into law and setting penalties for non-compliance enhances the power of deterrence of export control regulations. Besides, the introduction of such provisions is indicative of the intention of the legislator to emphasize on the responsibilities and the role that exporters could play in the oversight of sensitive trade activities. For example, exporters will be normally well-positioned in providing information to feed the risk analysis or a possible investigation conducted by the competent authorities, As Sevini notes, the highly technical nature of dual-use controls implies that, sometimes, only manufactures and users can easily assess whether their products meet the specifications of the control lists[327]. Besides, under Article 9 §2 of the EU regulation exporters are required to supply the competent authorities with complete information in particular on the end-user, the country of destination and the end-use in order to get an individual or global authorisation.

Firms and research organisations may be the first embankment before the release of a good or technology to an unlawful end-user. The adoption of ICPs is very important in this regard since they contribute to both the prevention and detection of export control violations[328].

European Union (2015): 614, retrieved from: http://bookshop.europa.eu/en/esarda-37th-annual-meeting-proceedings-pbLCNA27342/?CatalogCategoryID=fKcKABst.9kAAAEjqJAY4e5L.

[327] Ibid, 609.

[328] For an introduction to the role of ICPs see: South East and Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons (SEESAC), Internal Compliance Programmes, 2011.

Their usefulness can be greatly discerned when it comes to the control of ITT posing export control risks. The competent authorities may rely heavily on compliance measures and reporting done internally and sometimes voluntary by these companies committed to keeping track of all potentially sensitive information flows. Indeed, little would be effectively possible without informed, collaborative and compliant suppliers and exporters[329]'The WA Best Practices for Implementing ITT Controls' agreed back in 2006 recommend "the imposition of a requirement on industry, academia, and individuals to keep records, for an appropriate period of time, that clearly identify all controlled technology transferred, the dates between which it was transferred, and the identity of the end-user of all intangible transfers of technology for which licenses have been issued that may be inspected by, or otherwise provided to, export control authorities upon request". Given the practical and legal implications pertaining to the monitoring of ITT, internal measures are considered to be as an appropriate tool for responding to such export control challenges. For instance, record keeping and more comprehensive technology control plans seek to ensure that no risky ITT will take place and inadvertent or intentional attempts to transfer controlled technology will not remain undetected by either the company itself or the State authorities conducting compliance checks in the company in regular intervals.

In an ideal world, every company should have a compliance system in place with a view to conforming to the obligations set by the export control regulations. Despite the envisaged benefits, the implementation of ICPs does not constitute a legally binding obligation in most EU Member States. Yet, the practice shows that their implementation is taken into consideration during the examination of a license application.

Generally speaking, licensing authorities of different Member States expect from firms to have a sort of internal compliance mechanism albeit they do not necessarily require a full-fledged ICP. It is also recognised that compliance of SMEs poses a harsh challenge taking into account that numerous such firms are not even aware of their export control obligations. Licensing officers have a reasonable anticipation from exporters to know the technical specifications and the possible uses of the items to be exported as well as the identity of their customers including their respective business activities and needs. In turn, the competent authorities may take every possible step to render exporters aware of export control requirements, notify any amendments or new legislation introduced and, to provide assistance for the assessment of a doubtful transaction. For instance, the Business Danish Authority clarifies that "it is the responsibility of the exporter to make sure that their product is to be used in a civilian and peaceful context and to investigate whether specific exports of a product, a technology or technical assistance are subject to the export control rules". They add also that "although the responsibility for the decision rests with the exporter there are good opportunities for receiving advice and guidance from relevant authorities"[330]. The same approach is valid also in the USA where various government authorities provide guidelines

[329] Sevini et al. "Nuclear Suppliers' Enhanced Export Control Compliance and Communication with Authorities," 607.
[330] Danish Business Authority webpage on exporter's responsibilities, retrieved from: https://danishbusinessauthority.dk/exporters-responsibilities.

on what an ICP should cover clarifying, though, that the implementing decision is the sole responsibility of the individual companies. For instance, the US DOC has published comprehensive guidelines aimed at assisting companies to develop or improve their 'Export Management and Compliance Program' (EMCP) as ICPs are often called in the other side of Atlantic[331].

6.1.1 ICPs: a legally binding or a highly recommended instrument?

For some scholars and export control practitioners, internal compliance mechanisms should remain a non-legally binding requirement. Internal compliance is largely seen as a voluntary expression of the intention of the exporter to adhere to non-proliferation and other security imperatives. In another words, the company's hierarchy first and then all employees involved should see some merit in complying with trade controls if the effective implementation of ICPs is the purpose. Apart from that, it is often argued that implementing such programmes brings on additional costs and thus, a legally binding provision for introducing ICPs would pose an overwhelming economic burden to small and medium sized exporters, the backbone of the entrepreneurial activity in Europe. In relation to this, most Member States take into account the size of the firm and the degree of sensitivity of its activities when assessing an exporter's compliance system. For instance, the UK expects from large companies and regular exporters of controlled technology to have more formalised and comprehensive procedures, Hungary emphasizes the need for proportionate compliance measures and Denmark is careful not to harm the economic sustainability of small enterprises due to the imposition of adverse compliance requirements.

In addition, certain licensing officers highlight a crawling risk in setting formal ICP requirements: "ICPs could become a vague checklist that does not have much bearing on the culture of the company itself"[332]. Indeed, given the absence of EU wide guidelines for implementing ICPs and of certification procedures for compliant exporters, the mere fulfilment of formal checklists could result to unnecessary administrative burden for exporters and increased workload for the export control authorities. One could argue that is on the part of regulators to set benchmarks or minimum required standards for adopting ICPs usable by different types of exporters enabling thereby the consistent evaluation of such measures by the competent national authorities.

Establishing compliance requirements and a certification process for exporters ('suppliers') and end-users ('recipients') respectively of controlled items, software and technology is not completely unknown in the field of EU trade restrictions. The Directive 2009/43/EC is a

[331] US DOC, BIS, *Compliance Guidelines: How to develop an effective Export Management and Compliance Program and Manual*, 2011, retrieved from: http://www.bis.doc.gov/index.php/forms-documents/doc_view/7-compliance-guidelines.

[332] The information provided here derives from a survey on the implementation of ICPs and the interpretation of Article 12 of the dual-use regulation. The survey was conducted by the DG Trade in May 2011 and gathered responses from 16 Member States. The results were presented and further discussed in the framework of the DUCG (information retrieved from the Greek authorities). Although certain information might have changed since 2011, the survey is a good basis for drawing general conclusions on compliance practices followed by different EU Member States.

relevant example[333]. More particularly, the transfer of defence articles may be subject to restrictions also within the EU due to a Member State's essential security interests or on grounds of public policy or public security according to Articles 36 and 346 of the TFEU[334]. With a view to mitigating the impact of such restrictions on the internal market, the European Commission proposed, and the European Parliament and Council adopted the Directive 2009/43 "setting common rules and simplified procedures for the transfers of military equipment and its components to EU destinations". In practice, the directive sets out a license system allowing Member States to publish general licenses granting direct authorisation to compliant suppliers for the transfer of certain defence articles to certified recipients within the EU. Such licenses will be linked to certain conditions on the part of the suppliers such as a registration requirement prior the first use and record keeping obligations[335]. The certification of the recipients will be based on certain criteria proving their reliability (*e.g.* relevant industrial activity in defence products, commitment to compliance at senior level and implementation of ICPs).

> Member States shall designate competent authorities to carry out the certification of recipients established on their territory of defence-related products under transfer licences published by other Member States in accordance with Article 5(2) (b).
>
> *Article 9 §1 of the Directive 2009/43/EC*

In this regard, a subsequent Commission Recommendation draws from 'best practices' followed by certain Member States in this area and details minimum standards and common rules for the certification and monitoring of defence undertakings to be considered as 'eligible recipients' of controlled defence-related technologies[336]. The guidance elaborates the criteria referred to in article 9 of the Directive 2009/43 for assesing the reliability of recipients, clarifies the powers of competent authorities for monitoring compliance (*e.g*

[333] EU, *Directive 2009/43/EC of the European Parliament and the Council setting common rules and simplified procedures for the transfers of military equipment and its components to EU destinations*, Official Journal of the EU (L 146), Brussels, 2009.

[334] The Directive covers only certain defence-related products and their components derived from the EU Common Military List and specified in the Annex of the said Directive. Exceptionally, 'contracting authorities' (within the meaning of Article 1 of the Directive 2004/18/EC) purchasing defence-related products for exclusive use by the armed forces of a Member State may be entitled to receive such items without being certified. The Directive simplifying the transfers of defence-related items within the EU was set in force on 30th of June 2012.

[335] The directive provides also for global authorisations at request of a supplier. Article 7 specifies the cases where an individual license may be required:
(a) the request for a transfer licence is limited to one transfer;
(b) it is necessary for the protection of the essential security interests of the Member State or on grounds of public policy;
(c) it is necessary for compliance with international obligations and commitments of Member States; or,
(d) a Member State has serious reason to believe that the supplier will not be able to comply with all the terms and conditions necessary to grant it a global transfer licence.

[336] EU Commission, *Recommendation on the certification of defence undertakings under Article 9 of Directive 2009/43/EC*, Official Journal of the EU (L 11), 2011.

inspection visits and audits) and spells out the cases where corrective measures and suspension or revocation of certificates will be required. What is particularly interesting here is the Annex of the Recommendation containing detailed guidance on the key issues to be taken into consideration by the competent authorities when evaluating the compliacne perfomance of the recipients. The Annex consitutes a useful source of guidance for companies willing to deploy internal compliance measures. The core compliance areas enumerated in this guide are as follows:

- Organisational, human and technical resources allocated to the management of transfers and exports
- Chain of responsibility
- Internal audits
- General awareness raising
- Physical and technical security
- Record-keeping and traceability of exports and transfers

A plausible question here is whether a certification process or at least some common compliance standards could be established in the framework of dual-use export controls, as well. The certification of the recipients of dual-use commodities established outside the EU cannot be considered as a realistic scenario for practical and political reasons. The reverse that is to say the certification of compliant dual-use exporters based in the EU, could be an option; yet not the most fitted one. The scope of the Directive differs from the objectives of the dual-use regulation. The focus is on intra-EU transfers and defence articles. The number of companies concerned is considerably lower and the items in question of a more specific nature compared to the high number of exporters and the diverse range of products affected by dual-use export controls. Therefore, the certification of defence undertakings is a more straightforward and less resource-intensive process in relation to the certification of dual-use exporters[337]. That said, the establishment of minimum compliance standards could provide further impetus and useful assistance to exporters in meeting their ever increasing export control obligations.

In spite of the fact that the adoption of ICPs is not considered as a legally binding obligation, there is much talk in the EU circles about the implementation of Article 12 §2 of the Regulation stipulating the following:

"*When assessing an application for a global export authorisation Member States shall take into consideration the application by the exporter of proportionate and adequate means and procedures to ensure compliance with the provisions and objectives of this Regulation and with the terms and conditions of the authorisation*".

[337] In fact, even this ostensible simpler effort to eliminate obstacles, by creating essentially a common market in defence-related products, was not that successful. Rosanelli notes that national implementation was highly unharmonised, a fact that created doubts to European companies as regards the benefits of becoming certified. See Rosa Rosanelli, "Arms Export Controls- Setting Common International Standards," in *Modelling Dual-Use Trade Control Systems*, ed. Odette Jankowitsch-Prevor, Quentin Michel and Sylain Paile-Calvo. (Brussels: P.I.E. Peter Lang, 2014), 115.

It seems that the wording 'proportionate and adequate means and procedures to ensure compliance' leaves some space to different interpretations. On the one hand, there are scholars and policy-makers arguing that the article 12 alludes to a need for Member States authorities to require the implementation of ICPs by any exporter taking advantage of global licences. On the other hand, ICPs are not mentioned explicitly in the Regulation and some Member States challenge that ICPs are a necessary condition for the issuance of a global licence. Even though most Member States do not require specifically the implementation of ICPs for issuing global licenses, different Member States argue that: "ICPs or similar measures must be taken into consideration when assessing an application for global licenses, but Article 12 does not require ICPs to actually be put in place"[338]. Presumably the varying interpretations of article 12 are indicative of the way that internal compliance and ICPs are perceived by different Member States.

Furthermore, it seems that there is some degree of variation in practices followed by different EU Member States *vis-à-vis* internal compliance. For instance, some Member States attach also compliance requirements to general licenses other than global (NGAs, EU GEAs). Among them just few attach compliance requirements to individual licenses as well. In addition, the EU Member States rely on various means for monitoring the implementation of ICPs. In most countries the assessment of ICPs takes place under regular audits and sometimes through checks in the phase of the authorisation process or under the registration of new exporters.

In the same fashion, the specific form of requirements varies among different Member States. It may range from general criteria to be taken into account during the evaluation of an application to specific requirements laid down in the national law that is the most unlikely case. It is noteworthy that two of the very few Member States that used to have an ICP requirement enshrined in their national law, namely Poland and Hungary, they are going to withdraw such an obligation or, they have already done so. In Poland, exporters of dual-use items were required to implement ICPs according to ISO 9000 standard. Practically, this meant that a certified ICP had to be in place even for a single transfer of dual-use items. This was deemed as too restrictive especially for SMEs. Besides, this approach was departing from the obligations set in the Regulations and could possibly discourage exporters from applying for an export authorisation[339]. As a result, since May 2012, the law does not contain any longer such a requirement[340]. However, the Ministry of Foreign Affairs that is the advisory body engaged in the licensing process does take into account the implementation of ICPs prior to granting global licenses. In Hungary, the adoption of ICPs had been a legally binding obligation already for years before the entry into force of the dual-use regulation. However, under future legislation being currently in the pipeline, the implementation of ICPs

[338] See footnote 332.
[339] Information acquired after communication with Irena Kołakowska, expert at the Security Policy Department of the Polish Ministry of Foreign Affairs.
[340] It is noted that a certified ICP is still required for the transfers of defense articles. See the official note presenting the reasoning for the amendment of the law available in (polish): http://www.sejm.gov.pl/sejm7.nsf/druk.xsp?nr=229.

will remain a prerequisite only for the issuance of global licences. The Hungarian authorities deem that the conditions requiring the implementation of ICPs with regard to any type of authorisations have significantly changed[341]. The international environment has been evolved and the degree of awareness of exporters of dual-use items has been increased. Persistence to the fulfilment of rigid formal ICP requirements could mean unnecessary burden for both exporters and licensing authorities.

The lack of a homogenous approach on ICP requirements should not be seen as insufficient attention to compliance by the competent authorities. Germany for instance does not have a specific legal binding requirement in place for ICPs and nor does the UK. However, both Member States have published comprehensive guidelines and best practices for the implementation of ICPs by industry and both assess the ability of exporters to comply with export control rules during the application process[342]. In this regard, Members States may rely on more flexible and general provisions on restricted trade for the screening of compliant exporters during the assessment of an export application. For example, in Germany again, the general criterion on the 'reliability of the applicant' included in the Foreign Trade and Payment Act provides the legal basis for assessing the compliance status of dual-use exporters prior to granting an export authorisation[343]. Especially, for the granting of global licenses, the German export control authority investigate by means of written communication and on-site audits the adequacy of internal controls implemented by potential beneficiaries of such facilitations[344].

It turns out that the ICPs are understood -at least in the EU- as comprehensive procedures demanding increased investments in resources for both exporters and public administration. Member States prefer to maintain a flexible stance meaning that they strongly advise exporters to implement internal controls without setting explicitly legally binding requirements. In practice though, all governments do take into account the implementation of compliance measures by exporters. This way, EU authorities accept implicitly the voluntary

---

[341] Information acquired communication with the Head of the Hungarian licensing authority, Dr. L. Stefan, as of 1 April, 2015.

[342] UK Department for Business, Innovation & Skills, Export Control Organisation (ECO), *Compliance Code of Practice*, March, 2012, retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/341998/10-668-codepractice-compliance.pdf.
German Ministry for Economic Affairs and Energy, Federal Office for Economic Affairs and Export Control (BAFA), *Internal Compliance Programmes: Internal Export Control Systems*, June 2012, retrieved from: http://www.bafa.eu/bafa/en/export_control/publications/export_control_icp.pdf.

[343] The reliability of the exporters of restricted items will be assessed against certain criteria specified in the "Principles of the Federal Government for evaluating the reliability of exporters of war weapons and arms-related goods" as of 25 July, 2001 (document in German), retrieved from: http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/vorschriften/zuverlaessigkeit_ausfuhrverantwortlicher/index.html.
The main principles set concern the designation of staff responsible for export controls, the organisation of training for all employees involved, the definition of the chain of responsibility along the organisational structure of a company and the appropriate supervision to ensure that the predicted workflow is followed and ICP is functional (BAFA, "Internal Compliance Programmes" 2012, 11).

[344] German Ministry for Economic Affairs and Energy, BAFA, *Internal Compliance Programmes*, 10.

character of internal compliance measures and differentiate to some extent between full-fledged ICPs and other less comprehensive compliance mechanisms such as record keeping and export screening procedures. To conclude, maintaining some degree of flexibility in tuning ICP obligations and setting minimum standards at the EU level for implementing complete ICPs should not be seen as incompatible. Indeed, this could be a way forward for boosting export control compliance in the EU. The practice shows that different Member States have taken such actions at their respective jurisdictions by providing guidelines with key principles and basic elements to be incorporated and function in any ICP regardless of the exporters' size. For example, Denmark has developed standardised ICPs adaptable -with certain restrictions- to the situation of the exporter involved[345].

6.1.2 What is finally 'an internal compliance system'?

Although it would be more accurate to talk about internal compliance systems instead of internal compliance programmes the latter is most commonly used in Europe. ICPs reflect essentially procedures and mechanisms performing different functions and having as a common goal the fostering of a company's compliance with the export control law. As it will be explained later, such systems are usable for research organisations, too.

> An internal compliance system is an arrangement in which a company ensures that it is completing legal transactions, obeying the regulations enacted by the government, and fulfilling company export policies. Internal compliance systems typically include a set of procedures that company officials must satisfy before an item leaves the company. Such procedures include a thorough investigation of the buyer and end-user prior to the shipment of a purchased item off-site.
>
> *By the Institute for Science and International Security (ISIS)*[346]

What are the motives behind the introduction of ICPs by companies? Tangible benefits, compliance with legislation, fear of penalties and other liability costs, self-promotion of the organisation and furtherance of non-proliferation and other security objectives are the main drivers for adopting an ICP. More particularly, a sound compliance system paves the way for establishing a partnership between authorities and exporters. This 'trusted relationship' may be translated to palpable advantages for exporters in terms of simplified export procedures as discussed above. Moreover, it is such the nature of the export control law that exporters are required to keep a watchful eye on the legislation and pursue internal compliance measures. In relation to this, direct compliance requirements are also foreseen in the EU law. Article 20 of the dual-use Regulation sets a direct obligation for exporters and brokers of dual-use items to keep detailed records for at least 3 years and in accordance with the national law or practice in force in the Member State where they are established.

Failure to comply with the rules would mean administrative or criminal sanctions and other arduous consequences such as temporary suspension of exporting activities, lifting of trade

[345] See footnote 332.
[346] Definition retrieved from the Institute for Science and International Security available in: http://exportcontrols.info/key_elements.htm#models.

facilitations and blockade from markets. Member States may draw on different legal sources for enforcing effective, proportionate and dissuasive penalties against any export control violations. Such provisions may derive from national export control law or other corporate and civil law. In any case, article 24 of the Regulation provides the legal basis by stipulating that "each Member State shall take appropriate measures to ensure proper enforcement of all the provisions of this regulation".

> Each Member State shall take appropriate measures to ensure proper enforcement of all the provisions of this Regulation. In particular, it shall lay down the penalties applicable to infringements of the provisions of this regulation or of those adopted for its implementation. Those penalties must be effective, proportionate and dissuasive.
>
> *Article 24 of the regulation 428/2009*

Especially, for European firms the threat to lose markets in the US in case of poor compliance with obligations stemming from the US export control system is considered as a dissuasive factor. Also, falling short of requisite compliance standards or losing face due to lax implementation of the rules may harm the a company's good name and have implications for the whole country's exporting activities. For example, negative media attention can inflict a major blow to a company's reputation. "Even if a company is merely suspected of carrying out illegal export activities, its reputation in foreign trade may be tarnished"[347].

As some export compliance officers note fear and greed are frequently the two main motives driving compliance efforts of exporters. However, enhancing a company's corporate social responsibility and contributing to a safer and more secure world should not be underestimated. Companies and their employers may commit themselves to non-proliferation and national security imperatives once they realise what is at stake. No matter what is the motive behind (economic, moral, sense of responsibility) ICPs are arguably considered as an essential component of a company's trading strategy. In practice, exporters have strong interests to comply with the rules and export control authorities do take into account and encourage the implementation of such programmes. Table VI offers a summary of the benefits envisaged from the implementation of ICPs for both authorities and exporters.

Table VI: Benefits stemming from the implementation of ICPs

Reasons for requiring and implementing ICPs		
For export control authorities:	*For organisations:*	*Overall objective:*
Increased possibilities for identification of export control issues	Increased possibilities for informal inquiries	Exchanging of information and 'learning from each other'

[347] German Ministry for Economic Affairs and Energy, BAFA, *Internal Compliance Programmes*, 7.

Release of administrative work for non-cases	Economic benefits (*e.g.* simplified procedures)	Reducing operational costs
Ensuring compliance with challenging legislation (*e.g.* ITT controls)	Saving organisations from infringements and enhancing social responsibility	Furthering non-proliferation and foreign policy and security objectives
Identification of reliable exporters and optimisation of risk assessment	Detecting risky areas at an early stage and preventing risky transfers from taking place	Operating risk-based controls

What are main principles promoted by implementing ICPs and what are the 'standard' elements of an ICP? The 'European Code for Export Compliance', a private initiative undertaken by the 'European Institute for Export Compliance' highlights the main principles underpinning the operation of any robust export compliance system:[348] a.) Transparency b) Compliance c) Accountability d) Consistency and e) Effectiveness. An appropriate compliance system shall guarantee the transparent management of exporting activities, the delegation of clear responsibilities among the staff, the consistent pursuance and achievement of the set policies and objectives as well as the efficient and responsible use of the available resources. In the same code, 'export compliance' is defined as a specialised multidisciplinary framework providing support to organizations in managing export risks avoiding thereby legal and administrative sanctions, financial losses as well as reputation deterioration. It is also clarified that "export compliance covers all activities of import and export of goods and/or services, tangible and intangible assets (including the transfer of means of payment), that somehow are subject to regulations applicable to transactions between two different states/jurisdictions". This is not strange given that most of the time compliance systems in either academic or industrial organisations deal with the whole spectrum of export/import regulations.

> Monitoring and maintaining Export Compliance is [...] one of the most important methods for an organization to maintain its ethical health, support its long-term prosperity, and preserve and foster its values and avoid or mitigate any potential legal criminal proceedings.

[348] The 'EU Code of Export Compliance' (EU-CEC) is an initiative of a private organisation named as the 'European Institute for Export Compliance' (EIFEC) and providing export compliance guidance to public and private organisations. In alliance with its 'European Universities Network for Export Compliance' (EUNIFEC), EIFEC promotes the culture of sound export compliance practice, and accredits third parties to perform and enhance compliance professional activities. In doing so, it has also established the said code of conduct, an export compliance register for organisations and self-employed individuals engaged in the implementation of the EU Export control policy and even a certification process for compliant exporters. The EU-CEC can be accessed via this link: http://www.exportcompliance.eu/docs/eu_cec.pdf. For more information see the EIFEC website: http://www.exportcompliance.eu/index.php/en/about-eifec.

With regards to the specific elements of an ICP, guidance provided by government authorities in Europe and USA emphasize on the same key compliance components with slight differences each time (see figure below).

Figure VIII: "the internal compliance cycle"

1. *Management Commitment:* Commitment to compliance at senior level is important for symbolic and practical reasons or otherwise it is where compliance starts and most probably ends; if the senior management of an organisation is unaware of export compliance or does not see some added value in introducing an ICP, there will not be many chances for verifying and enhancing the export compliance status of the organisation. Generally speaking, senior management's commitment to compliance raises awareness within the organisation and it is the first step towards the creation of an export control culture[349]. In practical terms, most of the time it is a senior manager or the members of the directory board who carry any liabilities in the event of a breach of the civil or corporate law. For all these reasons, commitment to compliance by senior mangement should be expressed in written with a 'compliance statement' and shall be communicated to all employees (*e.g.* published to the orgnisation's intranet or sent by e-mail). The compliance statement should be signed by a person high in

[349] Sophany Ramaen, Filippo Sevini, Christos Charatsis, Michel Quentin, *JRC Technical Note on Strengthening Strategic Export Controls by Internal Compliance Programs*, Publications Office of the EU, Nuclear Security Unit, ITU, 2014, 7.

the hierarchy (*e.g.* by the 'Chief Executive Operator' in large firms) and it may be referred to in the organisation's mission statement.

2. *Appointment of a person in charge:* As it is the case with every management system, the responsibility for the operation of an ICP should lie with one individual nominated as the 'Export Compliance Manager' (EMC). The Wassenaar Arrangement 'best practice guidelines on ICPs' refer to the person supervising the development and functioning of a compliance programme as the 'Chief Export Control Officer' (CECO) pointing out also that he should be a senior representative director or other individual of corresponding status[350]. The EU Code of Conduct use the term 'Export Compliance Officer" (ECO) and further variations can be found. What is clear is that the seamless operation of an ICP requires the designation of a person as responsible for the development, implementation, monitoring and evaluation of the export control system always in conformity with the legislation and the needs of the organisation. Large exporters producing or trading regularly dual-use items or other controlled items have often several export control officers established in different business units and reporting centrally to the chief compliance officer. Export control responsibility will be assumed either as a stand-alone task by a dedicated structure *i.e.* an 'Export Control Unit' or as an additional task by an existing unit (*e.g.* a structure dealing with compliance in other areas). For some exporters –especially small and medium sized- the senior manager signing the compliance statement may be identical with the principal manager monitoring export compliance. Despite this, all available guidance highlights the importance of the independence of compliance mangers. "The main aim should be to protect export control staff, as far as possible, from any conflict of interests. There is, for example, a higher risk of conflicted interests if export control employees are also responsible for sales and marketing. For this reason, the export control department should be structured so that it is as independent as possible"[351]. Arguably, the fewer staff is available the more possibilities for conflict of interests may arise.

3. *Risk assessment:* 'Risk assessment' can be seen as an ongoing process taking place in different phases of the 'compliance cycle'. At first, introducing an ICP structure may demand a first 'mapping' of an organisation's sensitive activities, products and services against export control risks. A more thorough evaluation and rating of the products, parts and components, software and technology will take place in the phase of export screening procedures where specific risks are identified and mitigating measures are adopted. ICPs operate in a dynamic environment where risks should be determined or re-evaluated constantly and thus, export compliance depends on the evolving legal framework and the activities of a company or a research organisation undertaken each time.

4. *Written policy and manual with procedures:* Once a first risk evaluation has been conducted a formal compliance programme should be drafted. A written compliance

[350] WA, *Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies Guidelines*, 2011, 3. Retrieved from: http://www.wassenaar.org/guidelines/docs/2%20-%20Internal%20Compliance%20Programmes.pdf

[351] German Ministry for Economic Affairs and Energy, BAFA, *Internal Compliance Programmes*, 2012, 17.

programme will include and elaborate the main principles endorsed in the compliance statement. As a rule of thumb the main compliance policy explaining why export compliance is important and how it will be achieved in a given organisation should be clear, short and must be communicated to and easily perceived by all staff. Apart from employees directly concerned with the exporting process, the scope of controls is such that employees involved in design, development, engineering, research, purchasing, and maintenance and after sales service may also have a role to play in the view of export controls[352]. An ICP will include normally a compliance manual clarifying in greater detail the chain of responsibility, the step-by-step procedures to be taken in response of an export control risk as well as the rules and principles governing the functioning of the ICP: Who is responsible for what action? What procedures/mechanisms are applicable for given 'export scenarios'? How often and towards whom export control trainings should be performed? What are the standard operational procedures for dealing with a violation or a suspicion of violation? How often should audits take place and by who? How often or under what circumstances should the ICP be revised? Compliance manuals are expected to provide also information sources made available by export control authorities or other private entities and research institutes providing commentaries and insights in the area of export control.

Figure IX: "Drawing up an internal compliance manual"[353]

5. *Pre to post export screening:* Export screening procedures refer to checks to be performed by the designated employees in the pre-export and where applicable post-shipment phase in accordance with the export control manual and the related law. Export screening is the core of an ICP and it may include all these actions required for the verification and mitigation of

[352] Ramaen et al., *Strengthening Strategic Export Controls by Internal Compliance Programs*, 7.
[353] Figure from presentation "Elements of a Successful Export Management and Compliance Program" offered by T. Andrukonis (US BIS) at the 3rd Conference on the impact of export controls on higher education and scientific institutions, organised by the Association of University Export Control officers (AUEO), June 7-9, 2015, Washington DC.

export risks in conformity with the obligations set in the legislation. In the pre-licensing phase it is determined whether an item to be shipped is subject to any export restrictions. The classification of exported items, sofware and technologies must be done on the basis of applicable export regulations at European and national level including dual-use lists, sanctions/embargoes lists, military lists and where relevant other applicable lists by non-EU countries. Exporting firms are required anyway to conduct a rating of their products in oder to attribute them the appropriate code according to the Harmonised System Code (HSC), the common customs language administered by the WCO. As part of this process exporters could also identify items regulated under dual-use export controls[354]. Admittedly, product classification can be time consuming and expensive depending on the product portfolio and the number of items to be rated whereas small exporters may not even be aware of export control implications[355]. Export control authorities may provide support and in some cases on-line tools for assisitng exporters with the classification of their products.

What is to be exported is not the only question to ask; the end-use and end-user of an export are equally important factors as much as the final destination and the routing of an export[356]. Given this, the plausibility of the stated end-use (*e.g.* recipient's activties shall justify a given export) and the reliability of the end-user and/or of any middlemen involved in the export (lawfulness of recipients) are important factors to consider in assesing an export case. In addition, there might be some souces of suspicion usually called as 'red flags' to seek for. The Wassenaar Arrangement has published a non-exhaustive list of questions to be taken into account during the risk assessment of an export[357]:

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?

[354] In the EU, there is also the Customs Combined Nomenclature (CCN), a system of classification based on the HSC and defining in greater detail the exporting products. Dual-use items have their own coding system which does not always correspond to the CCN classification attributed to a product. In practical terms, for each CCN there is not necessarily one corresponding dual-use code making the correlation between the two systems a challenging exercise.
[355] Ramaen et al., *Strengthening Strategic Export Controls by Internal Compliance Programs*, 9.
[356] In relation to the end-use/end-user assessment Article 9 §2 of the EU regulation specifies that "exporters shall supply the competent authorities with all relevant information required for their applications for individual and global export authorisation so as to provide complete information to the national competent authorities in particular on the end-user, the country of destination and the end- use of the item exported. The authorisation may be subject, if appropriate, to an end-use statement".
[357] WA website, "List of Advisory Questions for Industry agreed at the 2003 Plenary". Retrieved from: http://www.wassenaar.org/wp-content/uploads/2015/06/Final_Questions_for_Industry.pdf.

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?

Non-listed items may undergo export restrictions as provided by the catch-all clause of the Regulation. Such restrictions will depend on the final destination, the end-use and end-user of the export transaction and this is also why pre-export checks have an extra usefulness. In the case of a doubtful transaction or suspicious case national authorities shall be consulted for further advice[358]. Whenever an authorisation is applicable certain conditions may apply including the provision of end-user assurances. As a consequence, in the post-shipment phase further checks and documentation may be required ensuring the delivery of a given item to a specific end-user in the quantity specified in the customs declaration and the conditions attached in the export license. For research organisations that do not export goods regulalry the focus of screening proceudres would logically be on trasfers of technology as well as the provision of technical assistance.

6. *Information and training:* This is another important component of a compliance system and a first step towards the establishment of an export control consciousness among the employees of an organisation. It is also an ongoing effort demanding sometimes considerable resources. As the European Code of Export Compliance mentions organisations need to update their 'export compliance knowledge-base regulalry' and certainly, when a change in legislation or un update in the lists is adopted[359]. Promoting awareness and providing trainings on a regular basis are of fundamental importance for the actual implementation of an ICP. Providing handy information in the right websites, targeting appropriately selected staff for training and communicating effectively export control risks can substantially upgrade the use of the tools and procedures being part of an ICP. In the author's view, no compliance system will ever be effective unless it is underpinned by a strong communication strategy[360].

7. *Record keeping:* Record keeping procedures is a prerequisite under the EU regulation and it is mentioned also in the Wassenaar Arrangement 'Best Practice Guidelines on ICPs'. Export related documents may include export licenses, end-use certificates, invoices and

[358] In fact, certain countries such as the US, they publish a 'denied parties list' or other 'watch' lists prohibiting or setting additional license obligations for given export transactions with entities prescribed under the lists.
[359] EIFEC, The 'EU Code of Export Compliance, 12.
[360] This statement is a product of the author's experience in designing information sessions and communicating export control objectives during his service at the JRC.

records of electronic transfers. Export compliance officers and private companies offering compliance solutions advise their client organisations to document every e-mail, phone-call or hard-copy relating to an export control case. This approach is beneficial in many ways to the compliance system of an organisation: it may benefit auditing procedures to take place in a later stage and the risk assessment of future export transactions. Most importantly, in the event of an unintended violation a database containing export records may prove the exporter's bona fide or compliance integrity saving or alleviating the organisation from severe legal consequences. Ideally, an electronic system should be in place for the effective registration of the cases. What data should be retained, by who and for how long, it should be also clarified in the ICP manual as well.

8. *Compliance monitoring and auditing*: With a view to identifying and resolving inconsistencies between written procedures and their actual implementation, an ICP should provide for a performance review process to take place in regular intervals. Auditing could be done internally or outsourced to a third party and in any case should include clear objecives and reviewable items to be evaluated. Ideally, auditors must not be involved in the export controls chain of responsibility and they should be educated about the peculiarities of export controls. For small exporters, self-auditing will indvertently represent the only option. The reuslts of the auditing may reveal areas requiring improvement and lead to the re-assessment or modification of certain procedures set in an ICP manual. Perfomance indicators may be established in order to measure and evaluate the effectiveness of an ICP.

9. *Handling potential violations*: Specific procedures for reporting and dealing with suspected export control violations should be established and made known to all staff potentially involved. The triptych 'report-respond-correct' is of central importnace in identifying and handling export control violations. First, clear instructions and escalation processes should be provided in the ICP manual. According to the US DOC, a safe environment should be ensured for employees raising questions and concerns about export compliance including an anonymous reporting mechanism[361]. Second, investigation procedures on the basis of set criteria and timeframes may be also available. Third, corrective actions including a possibility for voluntary disclosure to competent authorities, disciplinary measures and positive rewards for non-compliant and compliant employees respectively would be predicted as well.

6.2 Government – Exporters: from a regulation-based relationship to the establishment of a partnership

As explained in section 6.1 the introduction of ICPs is of interest to both authorities and exporters. Heretofore, the focus was on actions to be taken on the part of exporters. However, enhancing compliance with export control requirements should be part of a wider strategy of export control authorities to establish a trusted relationship with the exporters. This effort

[361] Presentation "Elements of a Successful Export Management and Compliance Program" by T. Andrukonis (US BIS) at the 3rd Conference on the impact of export controls on higher education and scientific institutions organised by AUEO, June 7-9, 2015, Washington DC.

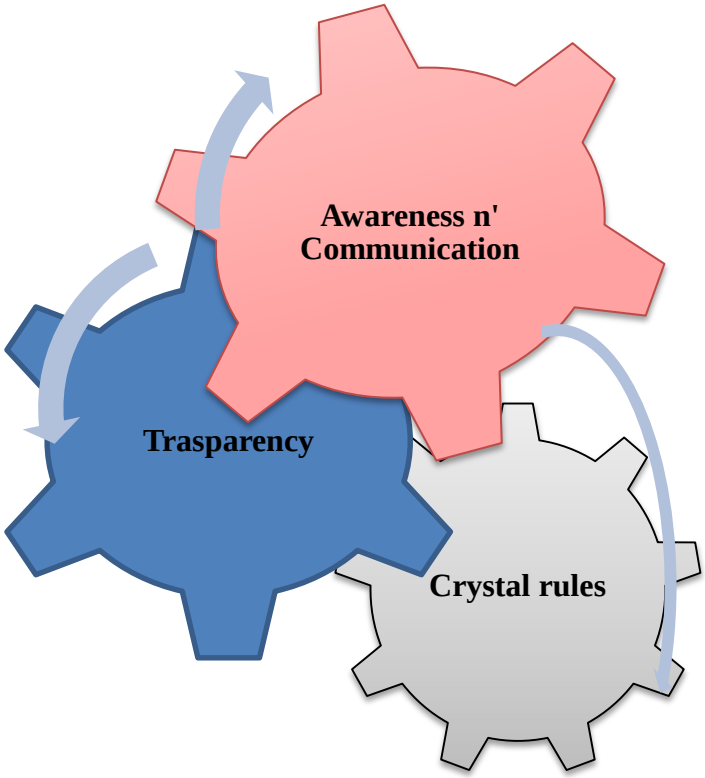
could comprise facilitating measures for reliable exporters, establishment of formal and informal channels of communication between the two parts as well as the provision of guidance and support such as trainings, guidelines and on-line tools readily available for registered or potential exporters of dual-use items and technologies.

> Effective State control of exports is only possible if all stakeholders, including manufacturers of critical goods, exporters, engineers, recognise the need for such controls and support them with all resources available to them. A close, trust-based partnership between industry and the authorities is vital if we are to achieve our shared objective.
>
> *German Federal German Ministry for Economic Affairs and Energy, BAFA 2012, 7*

Although the establishment of a trusted partnership and the attainment of a culture of open collaboration is a two-way relationship, regulatory authorities may have to establish the basis and the necessary conditions for the engagement of the private sector. Besides, export control authorities have anyway an interest to identify and reach out regular and potential exporters of dual-use technologies. In that respect, the role of authorities is similar to that of compliance officers trying to establish and consolidate an export control consciousness within an organisation. Communicating effectively the cause and main drivers behind the implementation of export controls such as non-proliferation and other security imperatives is an important element of awareness raising activities requiring a continuous effort on the part of authorities.

Second, promoting transparency of the licensing process by publishing for instance licensing data and clarifying applicable procedures to the extent permissible due to security limitations could further enhance trust to the authorities and export control processes in general. To that end, certain EU members States publish licensing data (*e.g.* the total number of general or individual authorisations by destination) through annual reports to the national parliaments or in the websites of the competent authorities. The degree of detail and the practices for collecting data may differ from State to State and actually, this is one of the reasons why the EU Commission could make only approximate estimations when publishing licensing data concerning the state of play of export controls in the EU. As part of an open, safe and effective communication plan, export control authorities could commit themselves not to disclose sensitive information or 'trade secrets' to unauthorised persons when processing export applications or, requiring information for risk assessment purposes. Establishing secure mechanisms for the exchange of such information between exporters and authorities could be a further option. A transparent and open decision-making including public consultations with stakeholders so as to give the word to the exporters is requisite for establishing communication channels and succeeding in non-proliferation objectives.

Figure X: Establishing a trusted partnership between regulators and exporters



Finally, it should not be overlooked that a comprehensive and robust legal framework could enhance both the effectiveness and the credibility of a trade control system. Setting clear rules and export control procedures as well as making available the requisite guidance and support to exporters could reinforce the collaboration between the two edges of the spectrum, represented by exporters and authorities. The design above illustrates vividly the interrelationship between the three main prerequisites for establishing a partnership between regulators and exporters and promoting export compliance.

6.3. Toward standardisation?

As discussed in section 6.1.1, the certification of 'eligible exporters' may constitute an option albeit not always the most desirable one. On the contrary, setting certain common standards for compliance with dual-use export controls may be a more fitted solution. In this case it should be up to the competent authorities to verify and monitor the compliance status of an exporter (*e.g.* through audits) prior to granting an individual authorisation, a general license or allow other simplified export procedures. Unlike other domains such as the regulation of nuclear energy or chemical agents, no law-based institution exists that oversees and sets international standards for strategic trade controls[362]. Existing guidance by different EU

[362] Sevini et al. "Nuclear Suppliers' Enhanced Export Control Compliance and Communication with Authorities," 607.

Member States and the Annex of the Recommendation 'on the certification of defence undertakings' are valuable sources of inspiration for establishing common guidelines at the EU level.

Nevertheless, establishing standards, certification procedures and systems for securing the whole 'supply chain' may pose another risk. As compliance professionals often stress there is a plethora of compliance programmes and systems originating from both governments and specific industry sectors concerning different aspects of the supply chain without being, however, mutually recognised and coordinated. "Cross governmental or cross industry implications are not usually considered when creating a new compliance system or standard, thus leading to likely duplication of compliance activities and confusion in areas not directly involved in the original concept of the programme or standard"[363]. Indeed, the potential burden is quite high if one considers the existence of adjacent systems set to deal with a variety of compliance obligations not strictly related to trade controls. In the EU for instance, the discussion to connect the Customs Authorised Economic Operator system (AEO) with export compliance requirements under Article 12 of the Regulation has been so far fruitless[364].

International standards for implementing management systems provide an insight into how efficient compliance systems should look like at least in terms of generic management. In that respect, the International Organisation for Standardisation (ISO), the world's largest developer of international standards provides -with ISO 19600- useful guidance for operating effective compliance systems in any organisational context[365]. Organisations have to operate in an increasingly regulated environment; apart from legally binding regulations, organisations may commit themselves to voluntary but internationally accepted standards and practices concerning almost every aspect of the functioning of an organisation. Such standards may include from technical requirements for the production of safe and quality products to best practice guidelines for good governance. ISO 22000 group of standards addressing food safety issues[366], ISO standards for the storage and transfer of certain

[363] Martin Palmer, "Improving the Integrity of the Global Supply Chain: Working with Compliant Business Partners," *Strategic Trade Review* 1 (2015): 118.

[364] The EU AEO system takes into account main aspects:

- Compliance with customs legislation and taxation rules and absence of criminal offences related to the economic activity
- Appropriate record keeping
- Financial solvency.
- Proven practical standards of competence or professional qualifications
- Appropriate security and safety measures.

For more information see the EU Taxation and Customs Union website, available in: http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/aeo_en.htm#what_is.

[365] The International Organization for Standardization (1946) is an independent, non-governmental membership organization with a long tradition in establishing internationally accepted standards. It has 162 member countries represented by their national standards bodies and it has published over 19.500 international standards in operation so far. For more information see the webpage of the organisation: http://www.iso.org/iso/home/about.htm.

[366] ISO 22000 - Food safety management, retrieved from:

dangerous goods[367], ISO 26000 on social responsibility[368], ISO 9000 for quality management[369] and ISO 31000 for risk management[370] are but few examples of famous ISO standards. ISO standards "provide a presumption of conformance with specific regulatory requirements" and in some instances are referenced by national regulations and UN recommendations[371].

As Makowicz suggests the establishment of ISO 19600 as a benchmark for implementing effective compliance systems may have some usefulness from a non-proliferation point of view, too[372]. According to ISO 19600 standards, 'compliance' means meeting all of an organisation's compliance obligations and hence, non-proliferation and more specifically export control requirements are one of these areas that can be dealt within the framework of a compliance management system. Organisations can voluntarily agree to adopt and abide by such standards and authorities may embrace standardisation by directly referring to or incorporating such standards into law. It follows that if it is judged as useful 19600 standards can be directly referenced to export control law at national, European or international level and competent authorities could take into consideration such standards when evaluating the effectiveness of compliance measures adopted by the exporters of dual-use goods.

Bearing in mind the key export compliance components referred to in section 6.1.2 and drawing from the main principles for effective compliance systems highlighted in ISO 19600 standards a more elaborate method for establishing and operating ICPs can be set. From the preamble it must be said that the compliance function should be as much independent as possible, it should have direct access to the top management or governing body and shall be given appropriate authority and adequate resources. Above all, continual monitoring and improvement is *sine qua non* for any management system devised to be efficient and effective. In that respect, every management project is set and implemented in four steps and therefore, it may be useful to determine four main phases for establishing and operating an ICP. The 'PDCA cycle' of continual improvement, also known as the "Plan-Do-Check-Act" principle, is the concept underpinning this four-phased management process and is referenced

---

http://www.iso.org/iso/home/standards/management-standards/iso22000.htm.

[367] For an example see ISO/TC 197 in the field of systems and devices for the production, storage, transport, measurement and use of hydrogen, retrieved from: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=54560.

[368] ISO 26000 – Social Responsibility, retrieved from: http://www.iso.org/iso/home/standards/iso26000.htm.

[369] ISO 9000 - Quality management, retrieved from: http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm.

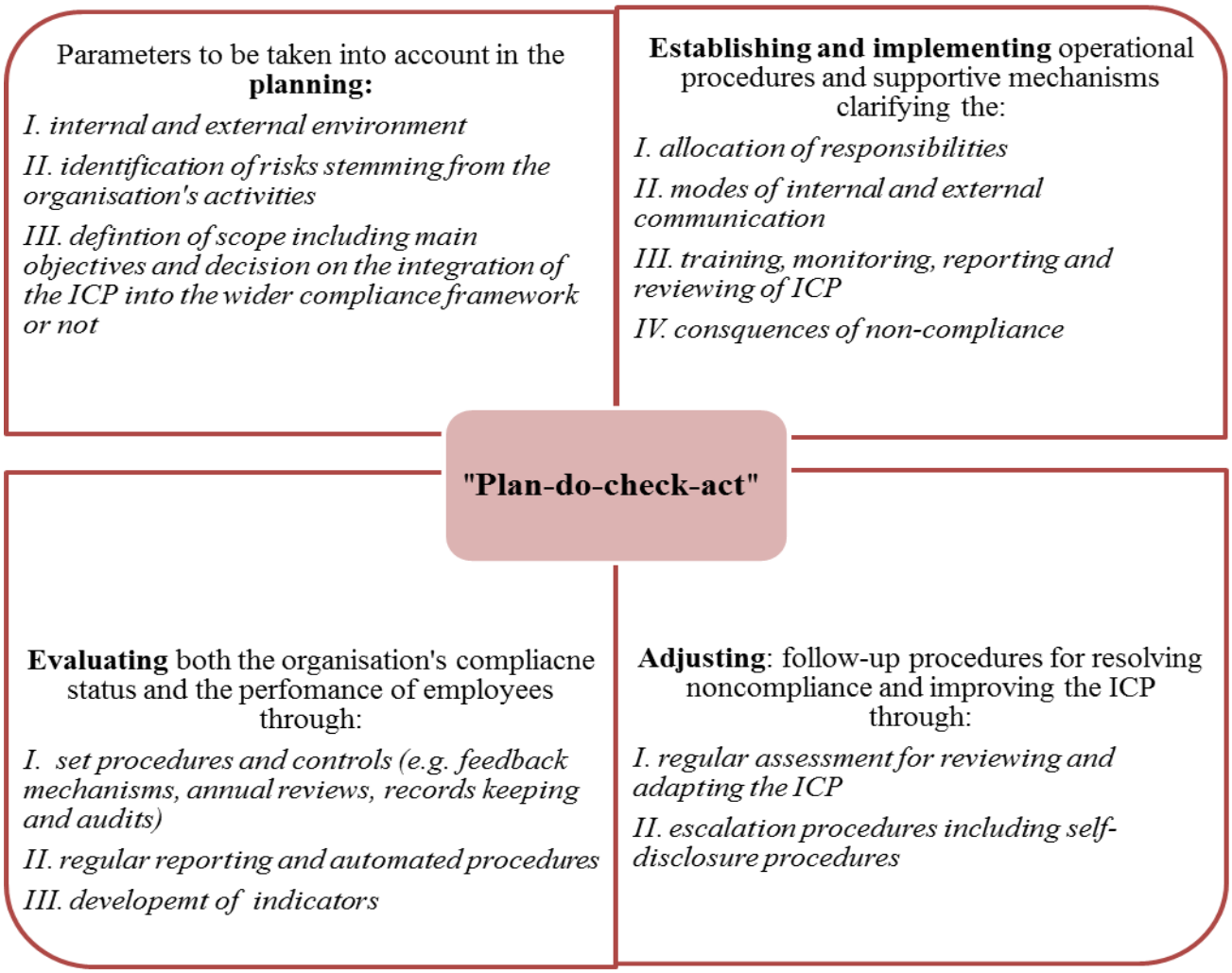
[370] ISO 31000- Risk Management, retrieved from: http://www.iso.org/iso/home/standards/iso31000.htm.

[371] For more information on the role of ISO standards in policy making please see the section of ISO website "Using and referencing ISO and IEC standards to support public policy" as of 2014, retrieved from: http://www.iso.org/sites/policy/index.html.

[372] Bartosz Makowicz, "ISO 19600 as Benchmark for Management of proliferation within an Integrated Compliance Management System," *1540 Compass* 8 (2015): 27-30, retrieved from: http://cits.uga.edu/uploads/1540compass/1540PDFs/compass%288v2%29.pdf.

also in ISO 19600[373]. The terms compliance system, or shorter ICP are interchangeably used in the following section.

Figure XI: A method for adopting and operating ICPs



I. Planning: Understanding the external and internal context of an organisation is the first step. An organisation should examine the requirements set in the related law as well as the broader conditions shaping its role and mission. An ICP will not be applied in a vacuum and thus, the identity of the organisation is certainly an important factor to take into account. Thereafter, a first identification of the export control risks stemming from the specific activities and transactions of the organisation would be necessary. The current organisation's functioning including institutional processes and activities needs to be evaluated against the legal obligations and any voluntary commitments undertaken by the organisation. The

[373] The PDCA cycle was originally developed by Walter Shewhart in 1940s, and it was popularized in 1950s by W. Edwards Deming. For an analysis of the evolution of the PDCA Cycle see: Ronald Moen and Clifford Norman, '"Circling Back: Clearing up myths about the Deming cycle and Seeing How it Keeps Evolving," Quality Progress, American Society for Quality, 2010, retrieved from: http://www.westga.edu/~dturner/PDCA.pdf.

ultimate goal for this phase will be to clarify the scope of the export compliance system setting main objectives and priorities as well as taking into account any limitation underlying its functioning. In addition, a central question to ask to be posed here is whether the export compliance system should be a stand-alone structure or incorporated in the existing compliance system of an organisation. Proliferation risks might be handled within an integrated compliance management framework or a separate 'non-proliferation management system'[374]. In this regard, ISO 19600 clarifies that the recommended standards are compatible with any management system and can be combined with other ISO standards such as those for risk management (ISO 31000), auditing (ISO 19011) and social responsibility (ISO 26000). No matter what option is deemed as more beneficial for each organisation, an ICP would logically necessitate some degree of central coordination.

II. Establishing and Implementing: The second phase concerns how the ICP will operate in practice. This is the core process in setting up and operating an ICP. It includes not only the establishment of main rules and standard operational procedures to be followed but also decisions on the specific mechanisms required for rendering the export compliance policy effective and the compliance procedures operational as described in the export compliance manual. The management of the organisation may rely on existing tools and channels where possible introducing new mechanisms only when there is no other more advantageous alternative. The allocation of responsibilities to management and other staff in higher and lower levels, the modes of internal and external communication as well as the details for training, monitoring, reporting and reviewing the system will be clarified at this stage. Furthermore, according to ISO 19600, any outsourcing of the organisation's activities does not absolve the organisation from subsequent compliance obligations. Due diligence *vis-à-vis* the compliance performance of third parties should be part of any compliance system and, from an export control standpoint, the verification of the identity of suppliers, clients and contractors is anyhow an important aspect of the risk assessment. As soon as all the decisions have been taken, the procedures have been established and the programme has been set in detail, the ICP will be tested in practice.

III. Evaluating: Ideally, as explained in section 6.1.2, the export compliance manual should envisage a monitoring process for evaluating the compliance status of an organisation and the modus operandi of the ICP *per se*. A problematic situation may be the result of neglect or deliberative abuse and it may indicate a defect of the system. To that effect, certain controls and procedures shall be established evaluating both the performance of the employees and the effectiveness of the compliance system itself. The evaluation process would rely on reporting mechanisms, annual reviews, internal and external audits promoting thereby the constant evaluation and improvement of the compliance system. The compliance course of the organisation should be tracked –through record keeping- and evaluated against certain criteria and principles. In that regard, the development of indicators may represent a useful action to take up. Such indicators could measure if and how feedback mechanisms are used, what are the employees' perceptions for the compliance system as well as the frequency of contacts

[374] Makowicz, "ISO 19600 as Benchmark for Management of Proliferation within an Integrated Compliance Management System," 28.

with regulators and the percentage of employees receiving training[375]. Also, detaching incompatible roles and responsibilities and inserting automated processes where possible is a key issue to consider. Evaluation measures should be also subject to periodical assessment for ensuring their continuing effectiveness and adherence to the evolving needs and requirements of the organisational and external context.

IV. Adjusting: Once certain needs or weaknesses have been identified follow–up actions shall be taken in order to improve the system and response to new or other less urgent risks. Given also that risks may be dynamic and the external environment may change rapidly, the system may need to be adapted in order to address new risks and needs. In any case, at the beginning the programme will fulfil certain priorities as decided in phase I. ISO 19600 clarifies that the risk-based approach to compliance management does not mean that for low risk situations, non-compliance is acceptable. Instead, organisations can initially direct attention and resources to higher risks having as ultimate goal to cover all compliance risks. It is also for this reason why a systematic risk assessment and monitoring of the ICP shall be conducted. Although corrective actions may be required including the redesign and improvement of certain elements of the system, failure to prevent or detect a one off noncompliance does not necessarily hint at an ineffective compliance system. Incidents of misconduct or actual violation of the law shall be reported to the top management and the competent authorities under the escalation processes and in the time frame predicted in the manual.

6.4 Infusing an export compliance culture

National guidance in the EU and the US emphasize the idea of incorporating export compliance in the culture of exporting organisations. Establishing and maintaining a culture of integrity and compliance is also mentioned in the ISO 19600 whereby compliance culture is defined as "values, ethics and beliefs that exist throughout an organisation and interact with the organisation's structures and control systems to produce behavioural norms that are conducive to compliance outcomes". Therefore, it seems that the ultimate goal of every compliance effort should be the development of a culture of awareness and responsibility within a given organisation. As discussed in chapter 2.3 organisational culture constitutes an integral part to the identity of every organisation and can be defined as "the shared, tacit assumptions that have come to be taken for granted and that determine the members' daily behaviour"[376]. It comes out that the concept of culture emphasizes the role of human factor and it has some pertinence to all different aspects of compliance. For instance, the behavioural patterns of management and employees can be most or least conducive to risks relating to security and safety and stemming from activities involving hazardous materials

[375] Examples of indicators mentioned in ISO 19600. For more information on the development of indicators and their categorisation into activity indictors, reactive and predictive indicators please see ISO 19600 standards.

[376] Professor Edgar Schein provided first this definition for introducing a now widely used model of organisational culture. Afterwards, the IAEA relied on this model for developing the concepts of nuclear safety and security. Information drawn from presentation done by Andrea Viski in the context of the seminar on export control technical issues: "Enhanced Dialogue and Best Practices for Export Compliance," organised jointly by the European Commission Joint Research Centre and the US DOE Argonne National Lab in Ispra, Italy, April, 22-23 2015.

and equipment. However, introducing new nuggets into and, changing the culture of an organisation requires time. The question on how to instil and consolidate a culture of responsibility should not be addressed only by organisations and individuals. Compliance efforts can be further enhanced or influenced by initiatives undertaken by states, international organisations and the civil society notably through the establishment of codes of conduct or certain standards to be achieved by individuals and organisations concerned[377].

The concept of culture is well known and developed in certain areas such as in the nuclear safety and security. In fact, the need for a cultural basis for nuclear safety was conceived first[378]. The IAEA in its 'Implementing Guide on Nuclear Security Culture' published as report No 7, refers to the interface between the two disciplines clarifying differences and similarities. Safety culture is defined as "that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance[379]. The nuclear security culture is defined as "the assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security"[380]. While both disciplines have as a common goal to protect human lives, society and the environment by considering the risk of inadvertent human error, the nuclear security places additional emphasis on deliberate acts. In that regard, the subordinate objectives of nuclear safety and security can be in some instances mutually exclusive. "For example, while for safety purposes it may be desirable to identify and quantify the amount and types of radiological/nuclear materials in a specific area or facility, from a security perspective this disclosure could increase the attractiveness of the site as a prospective terrorist target" [381]. Apart from the nuclear safety and security, the role of culture has some bearing also for those aspects covered under the CBRN initiatives, such as mitigation of and preparedness against risks related to chemical, biological, radiological and nuclear materials and agents. In this regard, the discussion in conceptualising and promoting a common and sustainable CBRN security culture is a recurrent topic in the relevant fora. As I. Khirpunov mentions building a security culture remains largely isolated in the different CBRN silos without sufficient horizontal communication. Therefore, ways to identify synergies and promote concerted cooperation should be stepped up[382].

---

[377] For instance, the Boticelli Project is such an example of an initiative launched by AREVA and other mostly nuclear related firms. The Project aims at bringing together compliant exporters willing to abide by and implement commonly agreed industry best practices.

[378] Terry Kuykendall, Igor Khripunov, "Examining the Interface Between Nuclear Security Culture and Nuclear Safety Culture," *1540 Compass* 8 (2015): 34, retrieved from: http://cits.uga.edu/uploads/1540compass/1540PDFs/compass%288v2%29.pdf.

[379] IAEA, "Nuclear Security Culture: Implementing Guide" (IAEA Nuclear Security Series No 7), Vienna, 2008, 5, retrieved from: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1347_web.pdf.

[380] Ibid, 3.

[381] Extract from Kuykendall and Khripunov, "Examining the Interface Between Nuclear Security Culture and Nuclear Safety Culture," 35.

[382] Igor Khripunov, Arthur Eyzaguirre, Jessica Alcorn, "A Blueprint of CBRN Security Culture," *1540 Compass* 2, (2012): 11, retrieved from:

In spite of the usefulness of culture for complying and achieving security and safety goals, similar attention has not been drawn in the area of trade controls. As pointed in the section 3.4, non-proliferation objectives and other security imperatives are furthered through a number of instruments in nuclear, biological and chemicals areas. These instruments include physical protection and safety measures as well as trade controls. Taking this into account, it is surprising that the discussion on applying a culture of responsibility has captured –in varying degrees- security and safety aspects but not trade controls. A. Viski has highlighted this paradox and borrowing from the concept of nuclear security culture suggests a definition of 'Strategic Trade Control Culture' as follows: "the assembly of characteristics, attitudes, and behaviour of individuals and institutions which serves as a means to support and enhance non-proliferation through strategic trade controls"[383].

One could further rely on the nuclear security culture for identifying the main features underpinning a culture of compliance in any given field. Drawing from the organisational culture, the model of the nuclear security culture pinpoints four main requirements for creating and boosting a culture of responsibility in an organisation. First of all, security culture is founded on a belief that a credible threat exists and that (nuclear) security is important. Second, some overarching principles such as motivation, leadership, commitment and responsibility should guide decisions and behaviour throughout the organisation. Third, effective management systems prioritising security and ensuring good and quality governance through well-developed policies, procedures and practices should be in place. Last, the behavioural patterns of top management and personnel should promote and enhance security through inclusive decision making, effective communication, vigilance and adherence to procedures. A questioning and responsible attitude on the part of the employees and a strong and exemplary behaviour on the part of leadership and management can be considered as key issues in establishing a security culture.

Although a culture of security can be clarified and further enhanced though national and international initiatives, the responsibility for achieving such a goal rests primarily upon the organisations and individuals. Personal dedication, accountability and understanding of all individuals engaged in any activity that has a bearing on the security of nuclear activities are important prerequisites for developing a strong nuclear security culture[384]. The active, visible, consistent and sustained commitment of the governing body, top management and middle management towards a common standard of behaviour is also highlighted in ISO 19600 as a requirement for developing a compliance culture. Essentially, all the elements and procedures described in the IAEA guidance for promoting and enhancing a nuclear security culture are linked with the key elements required for implementing effective compliance systems. This premise is supportive to the conclusion that the ultimate goal of an internal compliance system is the establishment and enhancement of a culture of responsibility, a culture of compliance. The deriving outcome is that 'compliance culture' is not another fuzzy term.

---

http://cits.uga.edu/uploads/1540compass/1540PDFs/compass2-03-khripunov.pdf.

[383] Andrea Viski, "Building Strategic Trade Control Culture: Toward a New Phase in Nonproliferation," *1540 Compass* 8 (2015): 39.

[384] IAEA, "Nuclear Security Culture: Implementing Guide," 5.

Although it has different aspects it relates to certain characteristics enabling the creation and furtherance of a culture of integrity and responsibility in a given organisation.

7. Looking into Internal Compliance Measures Implemented in Different Research Settings

Chapter 6 theorised the concept of export compliance emphasizing also the objective of achieving a culture of compliance in a given organisation. Furthermore, chapter 6 described the necessary steps and key elements for building and implementing ICPs on the basis of available guidance and standards provided by European and US export control authorities and the ISO organisation. The focus has been mainly on firms exporting items and technologies through tangible means albeit the measures discussed cover intangible transfers of technology and provision of services, too.

Given the ultimate objective of the study that is the elaboration and test of a basic method for identifying risks and designing compliance systems in a research context, this chapter intends to show how export compliance is perceived and implemented in different organisational settings: Section 7.1 concerns industrial R&D and firms' exporting activities, section 7.2 explores compliance practices followed by universities in the US and the EU and finally, section 7.3 examines the compliance system implemented by a US and a European research organisation. The main intent is to shed light in some fundamental or particularly challenging aspects concerning the design and implementation of export compliance systems.

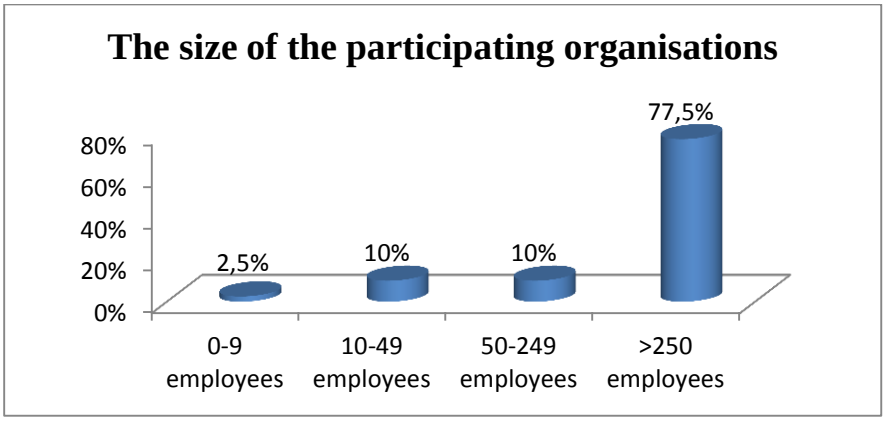
7.1 Complying with trade controls in an industrial setting

This section aims at presenting how different corporations deal with export controlled activities in practice. In doing so, current approaches, attitudes and practices *vis-à-vis* internal compliance including challenges and limitations are identified. The analysis examines certain aspects of export compliance in industrial settings. First, organisational and operational issues are addressed: what are the required resources for implementing an export compliance programme? How are duties and resources allocated to specific departments? What are the most resource-intensive tasks? Is it advisable to deal with export compliance through a stand-alone function or not? What are the corporate/institutional policies and departments that might be involved in the implementation of ICPs? Second, risk assessment practices followed by different organisations are discussed: What are the tools and methods used most commonly for identifying sensitive transactions? Third, it is examined how corporations comply with requirements to monitor technology transfers and especially intangible ones. This aspect is particularly interesting all the more due to the relevance of technology transfers to scientific activities. Fourth, the connections between academic research and industrial research are discussed not least due to the fact that different types of research may relate to distinct export control provisions and exemptions. This is not an exhaustive study of all key elements relating to the implementation of ICPs. For instance, the establishment of indicators for monitoring the effectiveness of ICPs or of mechanisms for correcting non-compliance are not of interest in this analysis.

The following analysis draws mainly from the results of an online survey which ran from December 9, 2015 to January 8, 2016[385]. In addition, supplementary interviews were conducted with industry representatives with a view to clarifying certain aspects of the issues in question. The survey was addressed to a total of 60 professionals working as export control officers in various exporting firms -operating in the EU- and public affair consultants representing such companies in the pertinent European industry associations and unions[386]. The target was to reach out to a satisfying number of export control practitioners so as to acquire a sample reliable enough for the purposes of this chapter. The goal was to explore how exporters of dual-use technologies comply with the EU regulation and ensuing national legislation in practice.

7.1.1 Organisational identity

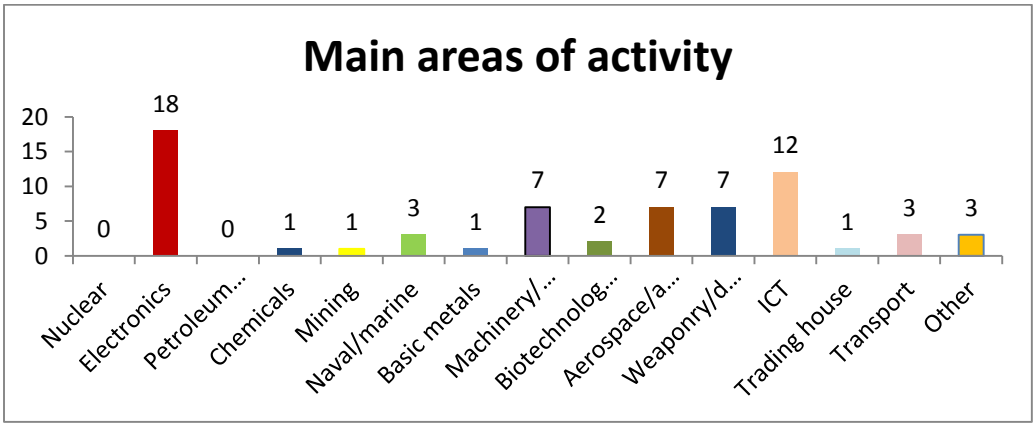
The survey gathered a total of 40 replies, a rather good response rate for the purpose of this chapter. The sample is made up mainly by large organisations (77%), a rather anticipated outcome given that ICPs are implemented primarily by large multinational companies undertaking exporting activities from different countries to diverse destinations. However, SMEs are also represented as well (22%). Almost all the respondents export items and/or technologies to both EU and non-EU destinations while 87% export also to the US.



The gathered data provide an insight into the compliance practices followed by companies operating mostly in the electronics, ICT, machine tools and aerospace/aviation sectors (in ranking sequence). Among the first things that the respondents were called to reply was their motivation for implementing compliance measures. Not surprisingly, administrative sanctions (*e.g.* fines, temporary suspension of exporting activities, lifting of trade facilitations) and reputational damage were the two most important motives gathering 32% and 22% respectively. Corporate Social Responsibility and criminal sanctions topped the replies as the least important drivers for implementing ICPs. This is also meaningful given that the case law in the EU has hardly to show any export control violations punished with imprisonment, and thus, a relation may exist between the low deterrence of criminal sanctions and their low ranking in the survey. It must be noted that criminal sanctions may involve both economic

[385] The survey was carried out in an anonymous way, the answers were provided on a voluntary basis and the data were treated in accordance with the applicable rules in the EU.
[386] Among the responding companies there is one conducting activities in the EU without maintaining a department in any of the EU Member States.

fines and imprisonment but proving criminality and bringing cases to the court seems to be quite a challenge[387]. In any case, economic sanctions such as suspending the exporting activities or business activities in general of a company or, imposing a fine seem to be effective deterrents. Additionally, certain factors are not disconnected; reputational damage and Corporate Social Responsibility is such an example. However, the way practitioners perceive and classify each motive may be indicative of the most prevailing attitudes encountered in an industrial context. Last, differences can be traced between SMEs and large companies. For SMEs, criminal sanctions and corporate responsibility stand as a medium driver for implementing compliance measures.



7.1.2 Compliance structure and resources

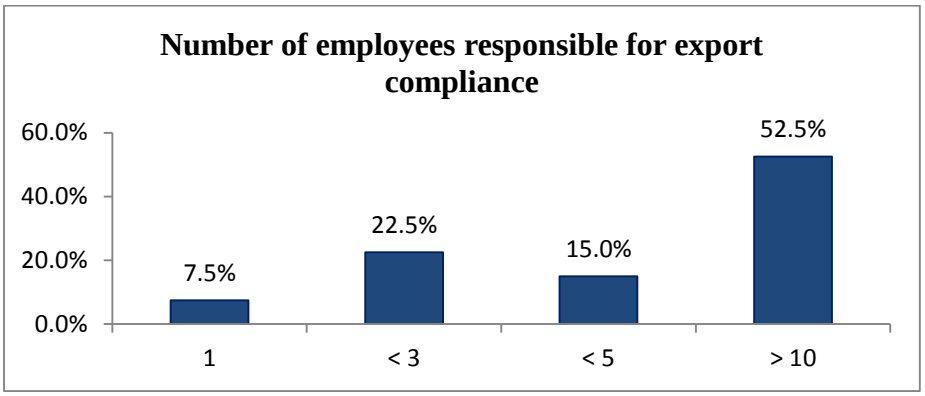
The great majority (87%) of the companies implement a formal ICP aimed at dealing with export control requirements whereas the rest implement a sort of individual compliance measures such as guidance material for sensitive exports and record keeping procedures[388]. The responses to the question whether export compliance is dealt with by a stand-alone system or not were divided with the positive exceeding slightly the negatives. 71% of those not possessing a stand-alone export control system address export compliance in the framework of a broader compliance system dealing with a variety of requirements, mainly import regulations, staff codes of conduct and safety rules. The rest delegates export compliance tasks to another department such as the Logistics department.

Depending on their organisational structure and the delegation of roles, the function assuming the overall responsibility for export compliance is the CEO or the board of directors in 53% of the firms. For the rest 22%, the Head of Export Compliance is the main responsible and 20% delegates the responsibility to another manager at senior level. Also, 67% of the

[387] For an analysis of the challenges in enforcing and prosecuting export control violations please see: Sibylle Bauer, "WMD-Related Dual-Use Trade Control Offences In The European Union: Penalties and Prosecutions," *EU Non-Proliferation Papers No. 30*, *EU Non-Proliferation Consortium* (2013): 1-15, retrieved from: http://www.sipri.org/research/disarmament/eu-consortium/publications/nonproliferation-paper-30.

[388] One organisation (a trading company) replied that it does implement neither a formal ICP nor any sort of internal compliance mechanisms and thus, was not allowed to proceed further with the survey.

respondents fully agree with the statement "the employee with main responsibility for export control compliance has direct access to top management (*e.g.* COE and governing board)".



Generally speaking, the majority (52%) of the responding organisations delegate export control roles to more than 10 employees. However, most of the time only a rather low percentage of staff assigned such a role is solely responsible for export compliance[389]. For SMEs the corresponding percentage is considerably lower (22%). The high number of employees contributing to export compliance tasks is a reasonable outcome, if one considers the high number of large enterprises participating in the survey. High numbers of employees must be translated to considerable resources dedicated to payroll and indeed, this is the situation depicted in the survey: 55% of the respondents chose staff expenses as the most costly aspect of their compliance mechanisms. Expenses for IT systems (*e.g.* for risk assessment, rating of items and recordkeeping) scored very high as well: 32% selected them as the most costly factor. The majority of export compliance officers consider training costs as a low to medium cost while half of them listed auditing as the least costly aspect of an ICP[390]. The figures are very similar for both large and medium sized enterprises.

7.1.3 Risk assessment and further operational issues

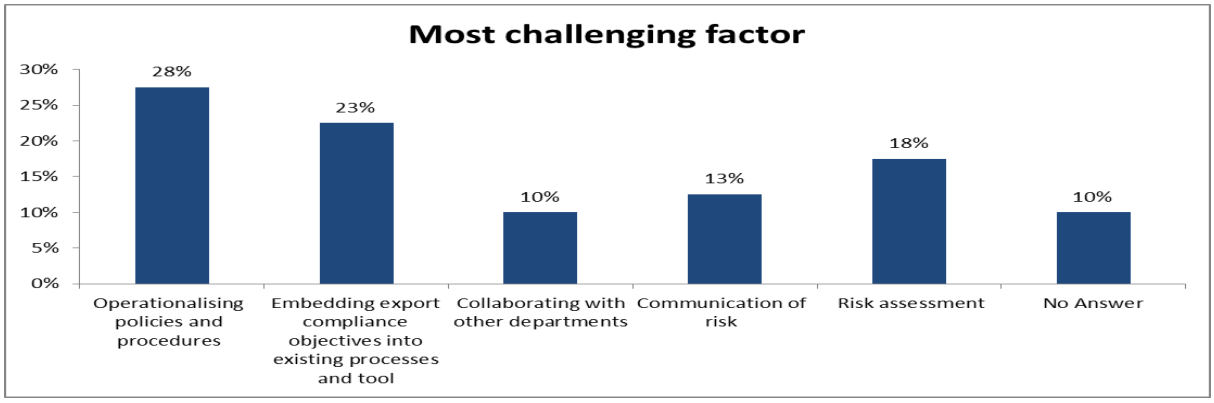
This section is particularly useful since it elucidates the different ways that companies of different sizes perceive challenges relating to the implementation of compliance systems. The section also exemplifies the different tools and practices used for identifying export control risks stemming from a given transaction.

The first question concerned the main challenges encountered in developing and implementing compliance mechanisms and fully-fledged ICPs. Although the replies are distributed in a quite balanced manner among the different available options, certain trends are identifiable. Operationalizing corporate policies and procedures and embedding export control objectives into existing processes and tools appear to be the most important

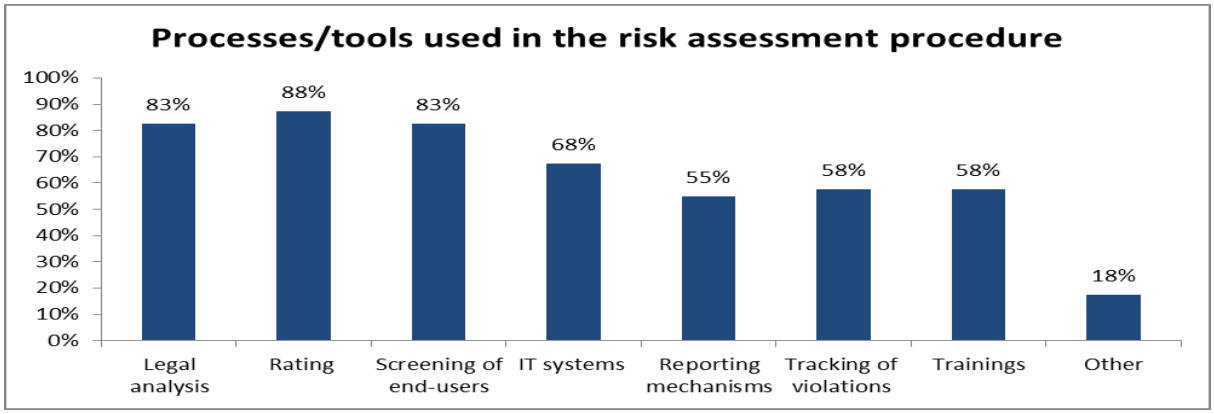
[389] There is the exception of some large companies having globally from 30 to 100 employees solely concerned with export compliance. One can assume that these companies export mostly controlled items and technologies and have subsidiaries in many countries.

[390] Auditing is usually addressed as in the context of broader auditing checks and this could indeed imply lower costs. Training costs might concern again staff costs plus material required for such and working hours invested. However, the questionnaire had no specific question on the criteria used for estimating compliance costs.

challenges. Actually for SMEs, the latter is the most important challenge presumably because smaller companies do not necessarily establish formal policies and procedures. The risk assessment process ranks in the third position as the most important challenge. This is particularly the case for SMEs, 33% of which chose risk assessment as the most challenging issue as opposed to 13% of large companies. Collaborating with other departments and communicating the risk to top management and all employees potentially concerned appear to be the least challenging issues. Reasonably, for firms investing resources to export compliance there must not be a great difficulty in communicating the importance of export control issues to top managers. The survey also illustrates some more sector specific trends. For instance, firms operating in weaponry/defence sector see communication of the risks as the least important issue.



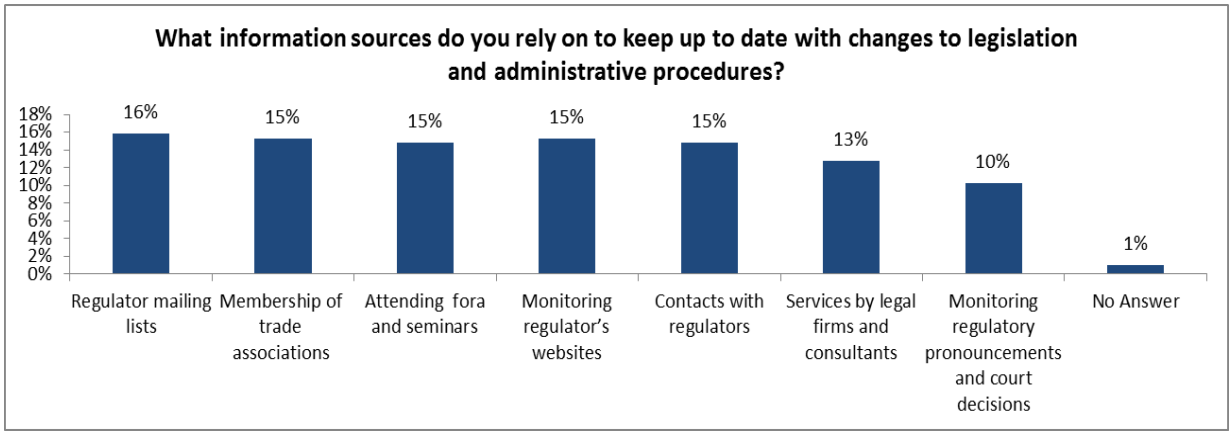
The second question concerned the processes and tools used in the risk assessment process. Rating exporting items and technologies against controlled lists, screening end-users and third parties against ban lists and analysing legal requirements are the methods used most commonly in the risk assessment. As far as it concerns the tools utilised, IT systems to manage, store, easily retrieve and share information were referred by 67% of respondents. Reporting mechanisms for notifying suspect cases, tracking of past violations as well as trainings are further sources feeding information to the risk assessment procedure for most of the firms. All the tools and processes achieve higher scores among large enterprises.



Most interestingly, some firms were willing to provide further information on the methods employed in assessing export control risks. For instance, one compliance officer singled out the specific steps followed in implementing a risk assessment process within an organisation.

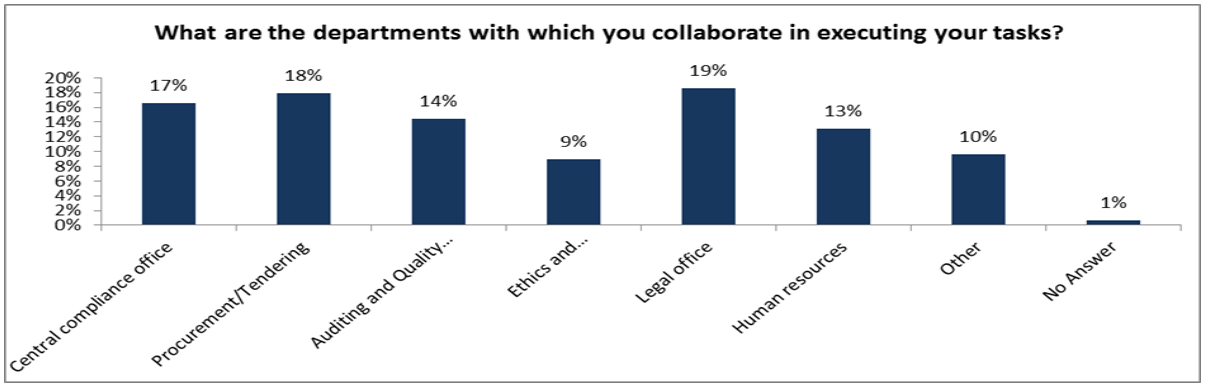
Building risk profiles (based on sensitive items, end-user/ end-use analysis, economic means of payment *etc.)* and identifying areas of risk are the first steps to be taken. Then, quantifying and prioritizing the risks and, identifying ways to address them are the next steps to take. Ultimately, implementing the necessary risk mitigation measures is the final step. Quite a few officers referred to self-assessment as a means used during the risk analysis. In practice, customers are required to fill out self-assessment forms which are then reviewed and classified by the export control officers. Also, risk assessment may involve contacting the customs authorities, asking for further information including patterns of sensitive transactions, routes and destinations. Enhanced risk mitigation measures may be foreseen for shipments going to sanctioned destinations.

Third, the participating practitioners were asked to list the information sources on which they rely so as to keep up to date with changes to legislation and administrative procedures and requirements. Despite the different resources and needs, retrieving information is enabled through a variety of tools for both SMEs and large enterprises. Subscribing to the authorities' mailing lists, attending export control fora and seminars and drawing information as members of trade associations and chambers of commerce are widespread practices especially among large firms. Monitoring regulators' websites, maintaining direct contacts with the licensing authority and participating to export control seminars are very common methods also for SMEs. It is also worth noting that 74% of the large firms and 22% of the SMEs rely also on private consultants and legal firms for dealing with export control requirements.



Fourth, the participants were called to answer what are the departments with which they collaborate in executing export compliance tasks. The legal office is the option gathering the most replies in the aggregate data. The Procurement and Tendering department rank first among the SMEs while the Central Compliance Office is among the first options in both large and medium sized enterprises. It seems also that companies -depending on their structure and needs- may collaborate with several other departments. Management processes relating to production, supply and sales of products such the Supply Chain Management, the Customer Relationship Management and the Product Life Cycle Management might have some relevance to export control tasks. Especially sales and customers support was quoted by quite a few practitioners. Moreover, the departments responsible for quality management, risk management and Corporate Social Responsibility and naturally, for R&D activities are further examples mentioned by few participants. Another question relevant to the previous

one was the following: "Can you identify other corporate policies that re-inforce export compliance?" Ethics rules (*e.g.* staff codes of conduct) and procedures for IT security are the two options gathering the majority of responses, 67% and 52% respectively. Quality management standards and classification policies for managing confidential information follow them with equal percentages each (45%). The procedures and checks established pursuant to the Authorised Economic Operators system (AEO) administered by customs authorities in the EU were referred to also as a 'reinforcing policy' in one case.



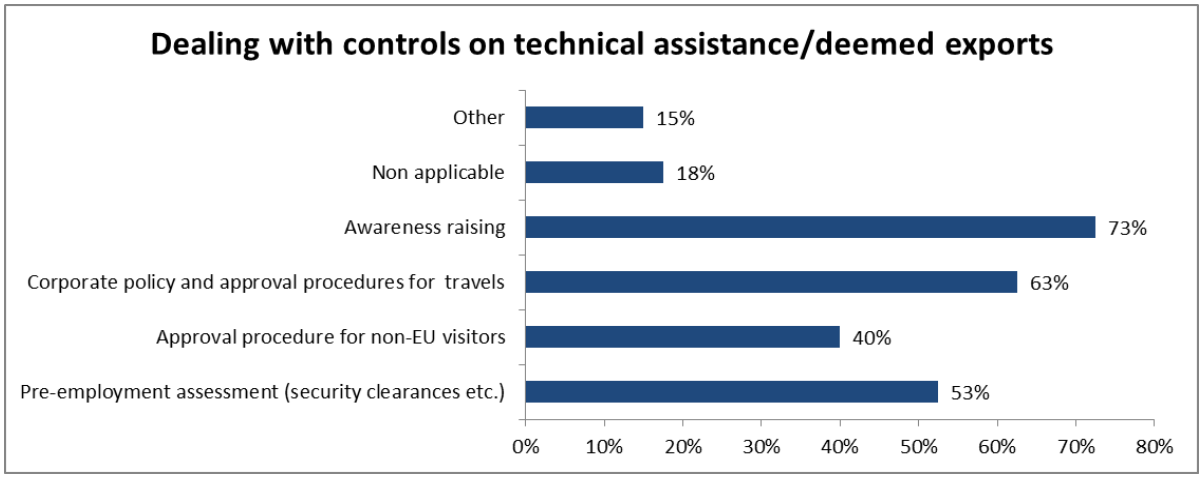
7.1.4 Monitoring Intangible Transfers of Technology

Complying with technology transfer requirements is considered to be as a major challenge and an issue of particular interest to this study. Generally speaking, large firms seem to be quite active in identifying and mitigating technology transfer risks. Technology transfers represent an important part of firms' business activities. Furthermore, quite often companies have anyhow an interest in controlling the sort of information that is released due to trade secrets and exclusive proprietary rights. If one thinks of the broad definition of technology as established in the framework of the multilateral regimes, corporations may transfer controlled technology in a number of occasions[391]. Transferring technical data to customers, sharing information with subsidies or collaborators abroad, and even sending data in the phase of tendering may be subject to licensing. Moreover, providing technical services outside the EU and releasing US origin information inside the EU may be subject to control under the EU Joint Action 2000/401 on the provision of technical assistance and the extraterritorial application of US deemed export controls, respectively. It must be reminded, however, that the EU technical assistance controls apply only in a narrow range of circumstances -military end-use- and deemed exports concern only US-origin technologies. Companies maintaining activities in particularly sensitive sectors and/or exporting technologies with military and defence applications such as aerospace and aviation may implement internal controls of very exhaustive nature.

Therefore, the survey seized the opportunity to explore the practices adopted by industry towards this issue. The first question was about the provision of technical assistance and the implications of deemed exports. 17% of the firms replied that they are not concerned by these

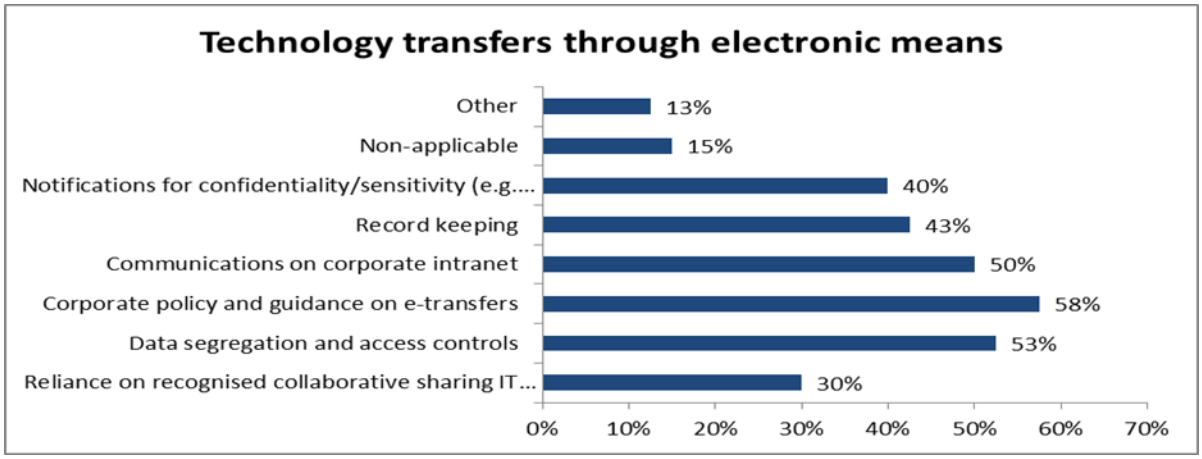
[391] It is reminded that technology is understood as the specific information necessary for the development, production or use of a product. The term information includes both technical data and technical assistance.

issues. Reasonably enough, the percentage of non-concerned firms is higher among SMEs (33%). Awareness raising activities are by far the most common tool referred to by most of the responding companies. Approval procedures for business travels abroad and pre-employment checks are among the elements used most in monitoring export related activities as well.



A few respondents referred to the different tools and management systems utilised in addressing tangible and intangible technology transfers. The release of export controlled information on-site is addressed mainly through the so-called 'Technology Control Plans' (TCPs) monitoring who has access to what information and ensuring that sensitive information is not exported to unauthorised users either on-site or abroad. Certain officers emphasized the role of visitor and travel management systems in operating effective TCPs. The application of deemed export/re-export rule may be translated into separate production lines or zoning excluding foreign employees from accessing certain US-origin technologies and information to use such technologies.

With regards to technology transfers enabled through electronic means, the responses are quite distributed among the different options suggested. However, the majority of firms have established a corporate policy and guidance for dealing with sensitive technology transfers. Data segregation and access controls as well as communications on the corporate intranet are among the practices used often for ensuring that sensitive information is not released to unauthorised users. Some export control officers highlighted the importance of monitoring planned technology transfers at an early stage so as to obtain required export licenses before such transfers take place. Relying on secure file transfer protocol and reliable file sharing platforms and, providing training to selected employees dealing with technology transfer most often are further tools mentioned.



With a view to understanding better the actual implementation of internal controls and evaluating the results of the survey, further inquiries were addressed to experienced compliance managers working for two leading MNCs. The following remarks concern, in the first place, companies exporting primarily controlled items and technologies and investing a lot of resources to export compliance. To begin with, such companies operate comprehensive corporate policies for dealing with technology transfers. The implementation of internal compliance policies requires the delegation of export control tasks to managers and local staff appointed in different units or business departments. Responding to the inquiries of employees concerned with export issues, approving export related transactions and submitting applications whenever an export authorisation is necessary are among their main responsibilities.

Second, in terms of risk assessment, prior to proceeding to any 'export' of technology certain information should be retrieved and analysed:

- the full description of the technology;
- the country of origin and any country that may exercise export control jurisdiction;
- the different places where technology will be moved to or accessed from;
- the end-uses and end-users relating to the transaction;
- the volume and value of export and,
- the involvement of any third parties in the provision or use of technology.

The rating of all exporting technologies demand both the attribution of the right Harmonised System Code and the verification of the export control classification number according to the respective lists applying for each jurisdiction when more than one are involved. The survey showed that for tangible goods a 'controlled item marking' is implemented by some companies. While the rating of items can be easily outsourced to customs brokers the classification of a technology requires *per force* an internal assessment. Internal assessments of potentially controlled items and technologies rely on tools and software provided either by external companies or developed in-house for this purpose[392]. Screening end-users and third

[392] In one case, a compliance officer described the system operated by his/her company as a 'tool' combining applicable legislation and corporate policies enabling thereby automatic export control objectives to be incorporated into companies processes and procedures. Whereas for intangible

parties against watch-lists and lists of restricted or sanctioned entities and individuals is integral to the risk assessment and due diligence process, as the survey confirms as well.

Furthermore, corporate policies can be quite exhaustive by covering all different occasions where a controlled technology transfer may take place and establishing export procedures to be followed. The interviewed officers confirmed that their firms' policies include physical exports of technologies, electronic technology transfers as well as transfers of hand-carried technology. For instance, travelling with laptops containing controlled data abroad can be subject to prior permit given that certain countries require an export authorisation for the export from or return of such data to the home-country of the employee[393]. In fact, in one case the company's policy provides for a special permit for taking IT equipment during business abroad. Another common practice confirmed also by the survey is that firms may require from their staff to use only the approved corporate file sharing platform for e-transfers. Yet, access restrictions may still apply since an export authorisation may be granted only for use by certain individuals located to certain destinations. In addition, different corporate policies set that transferring controlled data through e-mails should be as a last resort practice.

Given that governmental polices on technology transfer are still in development and therefore, sometimes incomplete, exporting firms may choose to undertake more strict and comprehensive rules than those explicitly provided in the law. This way they show in practice an attitude of responsibility and prevent inadvertent violations of the export control laws. For instance, so far there has been no formal guidance at the EU or at national level with regards to technology temporarily stored or accessed in servers abroad (see also chapter 4.2.2)[394]. However, and judging from the two inquires, the practice shows that corporate polices may address such a possibility. The responsible staff in collaboration with the IT department should be aware of the location of servers and data sharing applications used and report any export control issue, as appropriate. Last, keeping auditable records for each controlled technology transfer represents another main principle included in corporate policies and besides, it constitutes a formal requirement in the relevant law.

---

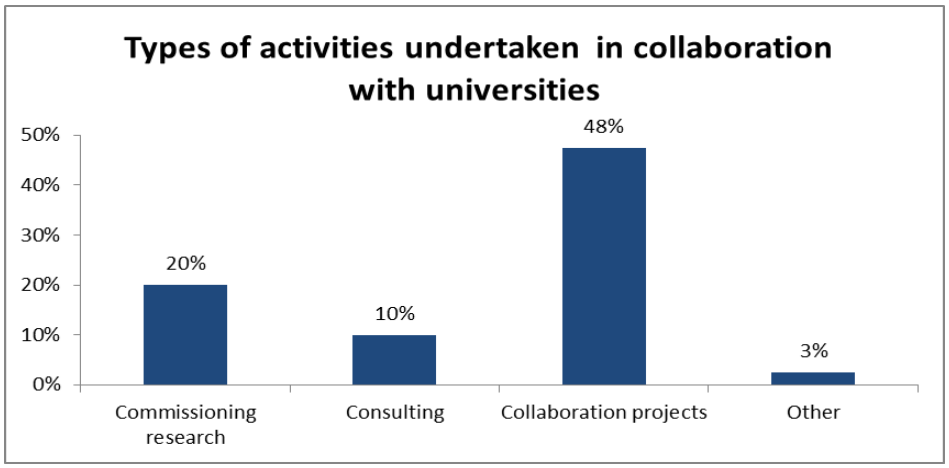
transfers an 'internal working council' is in charge for providing advice or ruling on the identification, classification and safeguarding of controlled information.

[393] The US is the most known case of a State requiring an authorisation also for controlled data contained in a laptop. On the contrary, the EU has not established a common rule on that issue. Article 7 of the dual-use regulation stipulates that cross-border movement of persons is not subject to export controls. For some Member States this provision implies that information contained in somebody's mind shall not be controlled. However, if an individual carries with him controlled information in a tangible electronic medium a license may be applicable. In sum, what shall apply in the case where controlled information is carried by an individual in tangible form such as laptops, USB flash drivers and portable hard disks has yet to be clarified (see also section 4.2).

[394] The issue has been discussed at the level of DUCG many times and interpretations of the applicable rules have been offered by certain Member States. However, common guiding rules have not been established so far.

7.1.5 Relations with academia and other research organisations

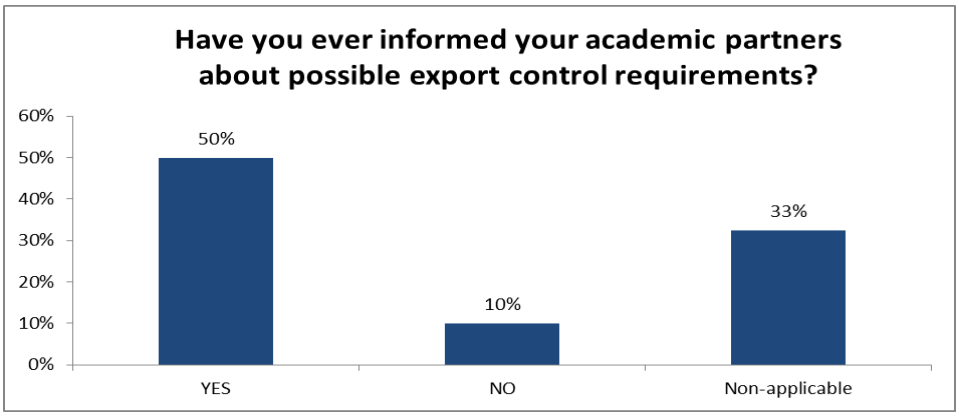
The concluding section of the survey was dedicated to the relations between industry and academic/research institutions. 57% of the respondents confirmed that they undertake research in collaboration with academia. Furthermore, 61% of those maintaining such relations with academia replied that export controls affect their cooperation with universities and other research institutes. For SMEs the picture is different since only 33% collaborates with academia and none of them sees export controls impacting this cooperation. The types of activities undertaken most commonly in partnership with academic and research organisations can be collaborating in joint projects, commissioning directly research to universities and, to a lesser extent requiring advice on given scientific issues.



The participants were also asked to explain how export controls affect their collaboration with academia. Most of them pointed out that technology transferred in the course of collaborative projects may be subject to an export authorisation. To quote just few of the officials, "we apply export controls in the same way as for other collaboration projects" and, "export licences are sometimes required to enable us to share data with research partners located outside the country of establishment." Moreover, technology developed may be controlled and thus, subject to authorisation. Information classified due to proprietary or security reasons warrants certain assurances and may require export authorisations as well. In that view, it might be also necessary for companies to ensure that their partners can only access those parts of their information systems that relate directly to the project in question and/or for which an export authorisation has been granted. "We have less flexibility when cooperating with research institutes based on certain destinations and, the US export controls may influence our decision to collaborate with some institutes due to deemed (re)exports," as another practitioner pointed out.

Quite interestingly, one official referred to the attitudes encountered in an academic context *vis-à-vis* export compliance. Sometimes research institutes are not aware of export control issues and researchers challenge the applicability of export control provisions as pursued through non-disclosure agreements. The survey asked export control officers to answer whether they have ever informed their academic partners about the applicability of export controls when transferring technologies, items and software. Half of the participants replied

that indeed they have done this before. It appears that industry may have also an important raising awareness role to play in enhancing compliance in a research environment.



Furthermore, a few officials stressed that collaborative projects either with subsidiary companies or with key suppliers may be obstructed due to delays in obtaining all the necessary licenses[395]. In that regard it is not only the interaction with academia that can be affected by export controls but also industrial R&D taking place within the framework of a multinational company. One officer referred to the lack of general licenses aimed at facilitating collaborative efforts both internally (within company) and with key suppliers. In that regard, the UK Export Control Organisation (ECO) pre-publishes a number of general licences which any exporting firm can make use of as long as it fulfils the specific conditions and is registered in the licensing database (SPIRE) set up for this purpose[396]. The idea to introduce new general licenses for intra-company transfers and large projects quite probably at the EU level is a long-lasting demand of the economic operators. Actually, the issue has been discussed in various occasions and studies in the past[397].

This doctoral study discussed the distinction between basic research and applied research in several occasions. Therefore, the survey participants were called to reply whether they

[395] To quote an officer, "In these cases, governmental approvals are needed to legitimately exchange export control data, even when such entities are controlled by the mother company and are covered by the mother company's ICP that is tailored in accordance to EU/US standards. Export license requirements have the potential to delay research projects."

[396] The (ECO) provides the possibility for using an OGEL allowing –subject to certain conditions- the export of dual-use technologies and software from the UK, or any other EU member state, where the exporter is established in the UK. For more information on the different types of general licenses available in the UK and their terms of use please see the website of the UK government in the following link: https://www.gov.uk/government/collections/open-general-export-licences-ogels#dual-use-open-general-export-licences.

[397] See for instance the Green Paper and the Staff Working Document report published as part of the consultation towards the review of the EU system: EU Commission, *Green paper: The dual-use export control system of the European Union: ensuring security and competitiveness in a changing world* COM(2011) 393 final, Brussels, 2011, retrieved from: http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf; *EU* Commission, *Staff Working Document, Strategic export controls: ensuring security and competitiveness in a changing world- A report on the public consultation launched under the Green Paper* SWD(2013) 7, Brussels, 2013, retrieved from: http://trade.ec.europa.eu/doclib/docs/2013/february/tradoc_150459.pdf.

conduct basic scientific research in the meaning of the EU regulation and, if yes, why. 25% of the participants replied that there are instances where they conduct basic research. If one extrapolates this figure to those undertaking research in partnership with the academia, the percentage rises to 43%. One could assume that companies have an interest in maintaining market leadership and their competitive advantages or to develop further their market position by investing in basic research and preparing the next generation of innovative technologies. In that sense, it is a meaningful fact that certain companies refused to provide further information on the instances where they conduct basic research. In one specific case the compliance officer said explicitly that this is secret information and, in another case, the reason referred to was 'striving for technology leadership'. Another interesting reply was the following: "the company maintains R&D facilities. Such facilities have the freedom to conduct basic research. The results of their scientific activities can be exploited by the company after further developments or can be provided to universities or research entities to nourish academic discourse." Last, one export control manager said that they conduct basic research only to the extent that this is a requirement of a government or an EU funded work programme. Last, one officer provided the example of legal studies commissioned to universities so as to understand better the obligations of transport sector in relation to export controls. Following this, a reasonable question to ask was whether there are cases where firms publish the results of their R&D activities in journals or other scientific publications. 42% of all firms questioned replied that they occasionally publish the results of their research[398].

In sum, the foregoing figures are useful in different ways. First, they confirm that firms undertake basic research and sometimes also publish the results of such research nourishing thereby the state of knowledge and public wellness. Second, they indicate that the interactions between academia and industry may be affected by export controls. It comes out that having a clear legal framework for determining where export controls apply as well as raising awareness within scientific organisations on possible export control issues could be of help. A hypothetical example could be helpful here: a pharmaceutical company conducts research for the development of a vaccine against a high pathogenic virus. In the course of the research the firm relies on inputs provided from and/or achieved through cooperation with a university. The exchanges concern technology that is necessary for the development, production and use of a listed virus. Are these exchanges bound to be subject to an export authorisation? Will the company be free to publish the outcomes of the research if it so decides ? This is a hypothetical case concerning a particular field of research but it is also an eloquent example of the issues at stake.

[398] If one extrapolates this figure to those collaborating with the academia the percentage will soar up to 74%.

7.2 University based research and trade controls

Discussing export compliance in a university setting is a challenging issue. Various experts and public authorities both in the US and the EU point out a number of difficulties in communicating export control risks and imperatives to the academic and scientific community. Officials from the DOC have noted that the initial efforts of US authorities -about 15 years ago- to reach out to a university audience were unsuccessful[399]. Only when they contacted those higher in rank (deans, faculty presidents), were they effective in building bridges of understanding and communicating trade control objectives to scientific staff and students. Hungarian licensing authorities were confronted with a similar attitude and a negative predisposition towards governmental controls of sensitive research during awareness raising seminars conducted in the past years in selected universities[400].

This is rather anticipated if one thinks of the distinct mind-set and practices pertaining to scientific research. Export controls are ostensibly at odds with the principles of academic freedom and independence of scientific work. On top of this, scientists may be unaware of export control risks and thus, they do not always realise how their work could connect to acts of WMD proliferation. Some of them will not be willing to carry further administrative burden and compliance checks if they do not see some merit in this. At the same time universities embark more and more often on partnerships with corporations and an increasing number of research projects are designed with a practical aim in view. As chapter 2 suggests tapping academic research into practical applications and furthering knowledge-based economies is favoured by governments and industry and, universities see in that an opportunity for funding their research programmes. Beside this, connecting the 'universitatum world' with the industrial world is not just about fundraising or commercial purposes. It might be also the means of responding to societal needs and translating a better understanding of the world to tangible benefits. This evolution takes place in an environment wherein the exchange of data and the flows of international students and professors is as high as ever. It is characteristic that quite a few universities organise and offer either free of charge or upon payment on-line courses and degrees and, operate international campuses in different countries or continents. Consequently, export control issues are intensified in such a context. This chapter intends to explore whether universities in the US and the EU are aware of export controls as well as what are their compliance practices for coping with the export control problem.

7.2.1 An insight into university export compliance in the US

US Universities are known to be pioneers across all university core missions -teaching, research, knowledge transfer and international outlook[401]. The USA is also a country with a

[399] Discussion with the Director of Office of Non-Proliferation and Treaty Compliance, A. Lopes, December 3, 2015.
[400] Discussion with Head of the Hungarian licensing authority, Dr. L. Stefan, September 24, 2015.
[401] If one looks for instance at the Times Higher Education World University Rankings or, the QS World University Rankings for 2015-2016 US universities such as the Massachusetts Institute of Technology, the Harvard, the Stanford University and the California Institute of Technology dominate the top 10 worldwide. Rankings available in:

long tradition in protecting intellectual property rights and implementing security controls especially for federally funded research. At the same time trade control legislation is generally considered as having a broader reach compared to the European one. In the US context, trade controls are openly seen to serve different objectives and the discussion is not limited to non-proliferation concerns. In addition to national security and international security objectives, protecting the US economic and technological advantages is a relevant aspect as well. Industrial espionage is an issue to consider in that regard. In various presentations and reports, US authorities stress that more than 56 foreign nations have been identified as collectors of US proprietary information and technologies. Among them 13 countries appear to be particularly aggressive collectors of U.S. proprietary economic information and critical technologies[402].

For many reasons, one could argue that US research institutions represent the one edge of the spectrum in terms of export compliance as opposed to EU universities that seem to be either unaware or less proactive. The analysis of the situation in the US relies on two different sources of information. The first is the insight acquired by the author during a conference organised by the Association of University Export Control Officers (AUECO), in June 2015[403]. This was the third annual conference organised by AUECO and gathered representatives from colleges and universities, speakers from government as well as private organisations specialised in global trade management and e-customs solutions. While this was just one of the numerous export control events and trainings offered to export compliance practitioners in the US, some remarks may be suitable here. The second source of information is the public university websites discussing exports compliance and providing documentation and advice to their staff for being compliant.

Overview of university compliance in the US: To begin with, the conference gathered export control compliance managers coming from over than 160 leading US universities such as the University of Stanford, the Princeton University, and the Columbia University. All

---

https://www.timeshighereducation.com/world-university-rankings/2016/world-ranking#!/page/0/length/25;
http://www.topuniversities.com/university-rankings/world-university-rankings/2015#sorting=rank+region=+country=+faculty=+stars=false+search=.

[402] Presentation by A. Lopes (US DOS), "The Nexus Between Strategic Trade Controls and Academic Research," December 3-4, 2015, Ispra;
For an overview of the impact of economic espionage in the US see indicatively (and its subsequent ones): US National Counterintelligence Center, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*," 1997, retrieved from: https://www.ncsc.gov/publications/reports/fecie_all/FECIE_1997.pdf.

[403] The AUECO in collaboration with the University of Virginia, the Virginia Polytechnic Institute and State University (Virginia Tech) and the George Mason University organised the third annual conference discussing export control compliance for universities and research organisations from 7 to 9 June 2015, in Washington DC. Presentations were offered by experienced university compliance officers, law experts as well as government officials from the Department of State, the Department of Commerce, the Department of Energy, the Department of Homeland Security and the Department of Treasury. Visual Compliance and Amber Road, private organisations offering global trade management and e-customs solutions, were the main sponsors of the conference. Information on the 3rd Annual Conference is available here: http://www.cpe.vt.edu/2015export/.
Information on the role and work of AUECO can be found in this link: http://aueco.org/.

these universities implement internal compliance measures and invest resources in so-called 'Export Management and Compliance Programmes'. This commitment of US academic institutions to export compliance may be attributed to various factors: increased awareness thanks to outreach activities by the US authorities; technological leadership and high intensity of knowledge transfers and, the rigorousness of the US export control law. This last element works in re-enforcement with a quite robust stance of authorities in enforcing export controls. During the three days of the conference, a number of university compliance officers referred several times to the verification or suspicion of export control violations as the main reason having led their institutions to adopt an export compliance strategy. It comes out that the preventive power of the US export controls towards universities is significant.

Despite that, it is estimated that from around 31.460 licences processed by BIS in 2014 only few concerned academic and research institutions[404]. In connection to this, there are not many known cases of violations involving academics. The website of the University of Pittsburgh refers to the most known export control violations recorded in the recent past[405]. The cited cases include both tangible and intangible transfers of controlled equipment and technology as well as the implementation of a catch-all control for equipment falling under EAR99 and sent to a restricted organisation specified in the Entity List. In 2009, the Georgia Institute of Technology made accessible restricted information to users in 36 countries, including China and Iran, by uploading such information on its servers. This is a telling example of an export control violation involving 'intangible transfers'. In 2004, a Professor of Texas Tech University received a 2 year prison sentence and a denial of his export privileges for a period of ten years for having illegally exported a controlled pathogen (the causative agent of human plague) to Tanzania. The most known case is probably the one concerning J. Reece Roth, Professor Emeritus at the University of Tennessee. Between January 2004 and May 2006, Professor Roth engaged in a conspiracy to transmit export controlled technical data subject to the ITAR to graduate students from China and Iran[406]. Although Roth claimed he was ignorant of the regulations, in practice he was warned on a number of occasions, including by university counsel, that the technology may have been controlled. Professor Roth was convicted in a four-year sentence.

The BIS Office of Export Enforcement (OEE) publication 'Do not Let This Happen to You' refers to further cases of violations and it notes also the role of Voluntary Self-Disclosures (VSD). Most of the VSD cases are closed with the issuance of a warning letter, some require no action and only very few lead to administrative sanctions. During 2014, the OEE opened a

[404] According to US authorities only a small percentage of licenses concern US universities and research organisations. For the total numbers of licenses processed, approved and denied please see Statistics of 2014 License Authorisations in the BIS website: https://www.bis.doc.gov/index.php/forms-documents/doc_view/1266-2014-statistical-analysis-of-bis-licensing.

[405] For more information please consult the website of the University of Pittsburgh, available in: http://www.export.pitt.edu/export-violations

[406] US DOS (BIS), Office of Export Enforcement, "Do not let this happen to you, Actual Investigations of Export Control and Anti-boycott Violations," 2015, 53, retrieved from: http://www.bis.doc.gov/index.php/forms-documents/doc_view/1005-don-t-let-this-happen-to-you-071814.

total of 312 VSD cases and closed a total of 213 VSD cases. Over half of these VSD cases were closed with the issuance of a warning letter, while nearly a third were closed with 'no action' or 'no violation' and, around three percent, were closed with the issuance of administrative sanctions[407]. The role of VSD in the implementation of compliance systems was underlined also during the conference. In case of an export violation, the implementation of compliance measures is among the factors taken into account in the prosecution of such violations and may attenuate an applicable penalty. US universities see in that a further motive for being proactive and complying with export controls.

Organisational and risk assessment aspects: With regards to organisational and operational aspects of export compliance in US academic settings, it could be difficult to build general patters and draw conclusions applying to all universities. The organisational structure may differ from one university to another and so does the scope of research activities concerned. This also implies that different universities employ compliance systems in a way that better fits their needs and identity. No matter where the export compliance function is placed, integrating export control objectives throughout the organisation is a key to implementing effective compliance systems. Mark Peters, an experienced compliance officer at Oregon State University (OSU) has noted that "for a standalone export compliance system, it would be very difficult to get the user's attention; however, if presented as part of shipping or dangerous goods compliance it receives much more attention and buy in. Additionally, researchers appreciate having the obstacle to research packaged together with a method to comply with all applicable regulations and move on their work"[408]. What's more, by working with other compliance operations, a university compliance officer develops a network that can provide insights into what institutional operations or specific projects may need attention from an export controls perspective. "These partner compliance departments become 'gate keepers' looking for problems and referring them to the export compliance staff". Moreover, other compliance officers highlight a difficulty to estimate staff hours and resources dedicated in assessing export control risks due to this involvement of staff from different departments.

Generally speaking, the Export Control Office (ECO) of an American University deals with the whole spectrum of prohibitions and restrictions from arms controls in defence related articles to controls of dual-use commodities and technologies and, from trade sanctions to anti-boycott and anti-corruption regulations. According to Mr. Peters, an export compliance programme takes about 2 years to get integrated into a US academic institution. The main challenge is creating awareness of the program and communicating to the faculty and staff the importance to seek assistance when an issue arise. The long time to implement a compliance system has as much to do with the traditional culture of openness in academia as with the complexity of the material.

[407] Ibid, p.9.
[408] Discussion in the margins of the AUECO conference and e-mail exchange with M. Peters, compliance officer at Oregon State University (OSU).

The AUECO has provided some guidance –a sort of basic model- for assessing a university's institutional structure, core competences and scope of activities against export control risks[409]. The main idea is to assess different aspects of each parameter referred above against given risk descriptors. For instance, the institutional structure of a university includes processes for budget allocation, compliance, purchasing, shipping and international travel. The extent to which such processes are centralized or distributed (risk descriptor) may indicate a higher or lower risk. The physical location(s) is also a relevant characteristic in this evaluation. According to the model, centralised procedures imply a lower risk.

The second parameter concerns research policies and core competencies of a research institution. For instance, a university implementing a policy of non-involvement to military/ defence related research or, refusing to undertake research involving non-disclosure agreements may be confronted with lower export control risks. Determining whether controlled or sensitive items (*e.g.* EAR and ITAR items and select agents) relate to the university core competences is part of the risk assessment, too. Focusing efforts on primary areas of concern such as nuclear, engineering, and biotechnology is a plausible practice to follow. Visibly, universities operating nuclear facilities and using special nuclear material face a higher possibility to be concerned by export controls. In author's view, the evaluation of the sensitivity research warrants an in depth and thorough examination given that less evident research activities (*e.g.* software simulating certain processes) may be also exploited by a proliferator or malevolent user for malign purposes and might be included in the scope of trade control lists. As M. Peters neatly notes, providing more and deeper education to researchers on export control issues represents a great way to mitigate export risks associating with a given discipline.

The third parameter that determines an export control risk is the scope of international activities undertaken by a university. Again here, every type of activity (collaborations, field research, operation of international campuses, student exchange programmes, online and distance learning) undertaken by a university can be classified as of low, moderate or high risk depending on a given risk descriptor. For instance, field research using EAR99 equipment shipped by a freight forwarder to low risk countries is considered as low risk activity. However, field research in a high risk country involving hand carried equipment that is not EAR99 may be of high risk. It can be concluded that one needs to correlate the results of risk assessment for different parameters (*e.g.* core competences within the scope of international activities involved) in order to identify and address specific export control risks.

M. Peters suggests a practical way for addressing first the most urgent risks and turn then attention to other less evident or urgent areas of concern within an institution. Simply put, "using a sliding scale, based upon research subject, amount of foreign participation and

[409] D. Brady, E. Peloso and G. Rowold -university compliance officers and members of AUECO- have built a risk assessment tool for classifying a university's institutional structure, core competencies and scope of international activities as of low, moderate or high risk. The tool was originally produced for use at the 54th Annual Meeting of the National Council of University Research Administrators (NCURA), November 3, 2012.

international collaboration along with reviewing funding source requirements allows for areas of greatest exposure to be reviewed first."

Technology Control Plans: Monitoring technology transfers poses probably the harshest challenge in implementing an export compliance system. In that regard, and given the extra complexity of the US export controls (think of deemed exports), it is interesting to see what measures are taken by the US universities in response to such legal requirements. A term used quite often when the discussion touches upon intangible transfers of technology is 'Technology Control Plans' (TCPs). Industrial operators have been implementing such measures for years as a means to protect classified, proprietary, and export-controlled information. In fact, TCPs are explicitly required or recommended by federal guidance and regulations dealing with sensitive information released during or produced by defense-related R&D[410]. In addition, the application of TCPs is a widely used export compliance practice adopted by all major US universities. The University of Washington (UW), for example, defines a TCP as an internal compliance document prepared by the responsible lead researcher and stating the type of export-controlled information associated with a research project as well as measures to be taken to ensure that access to export-controlled information is duly managed, and signed[411]. The approval of such TCPs lies normally with the university Export Control Office (ECO) that in the case of the UW is the Office of Sponsored Programs. Generally speaking, a TCP should deal with all different aspects of security and establish level access controls to laboratories, IT services and data[412]:

- physical security (*e.g.* security perimeter, safe storage and restricted access);
- information security (marking of e-documents, secure file transfer method *etc.*);
- specific procedures for any export authorisations required;
- personnel screening and foreign visitors' checks;
- training of authorised persons prior to receiving access rights;
- and record keeping.

[410] The National Industrial Security Program Operating Manual (NISPOM) and the ITAR are such examples. For an introduction to the role of TCPs see: Michael Swansburg, "Technology Control Plan," *Counterintelligence News and Developments* 1, 2000, available in: http://www.disam.dsca.mil/pubs/v.23_1/swansburg.pdf

[411] The UW website clarifies when a TCP is required:

- Projects or activities involve the receipt of Sensitive Unclassified Information (SUI) from an outside party or sponsor, such as via a nondisclosure agreement or sponsored research agreement;
- Projects or activities are not considered Fundamental Research;
- Projects or activities involve technology and software associated with export-controlled equipment.

For further information please consult the following link: https://www.washington.edu/research/?page=ecrTCP.

[412] See for instance presentation by Mary Beran (Georgia Tech) and David Brady (Virginia Tec): "Using Technology Control Plans in Export Compliance," University of Pennsylvania (Office of Research Services), available in: http://www.upenn.edu/researchservices/Export%20Controls%20Conference/Mary%20Beran%20&%20David%20Brady%20-%20Using%20Technology%20Control%20Plans%20in%20Export%20Compliance.pdf.

Furthermore, several presentations made available in the Universities' websites include 'management commitment to export compliance' as an essential element of an effective TCP. The University of Virginia (UOV) stipulates in its export control policy that "Faculty members wishing to use (or authorize students or staff to use) controlled technology or work on a project intended to generate controlled technology, regardless of funding source, must develop a TCP"[413]. The TCP should be adapted to the specific needs and implications of a given project and receive approval by the OEC. The OEC may decide that a TCP is not required for instance in the case where a project involves merely tangible transfers of EAR-controlled items, does not concern controlled source code or proprietary technical information and the research is to be conducted exclusively in the US. Similar procedures for monitoring sensitive projects involving intangible transfers of information are implemented by several US Universities. One could say that TCPs are like targeted ICPs incorporated in broader export compliance management systems.

Further Common Elements: The investigation in the websites of different US universities showed certain elements that are in common for most of them. First, the majority of the US universities take export compliance quite seriously and to that effect, they have adopted a proactive stance. More particularly, several US Universities provide basic information on US export control regulations, guidance manuals and policy statements. The UOV that was referred above is such an example of a university having established quite comprehensive policies and procedures. For example, the UOV policy on sanctions requires that: "all University activities that are to be conducted in, involve the participation of parties located in, or will benefit a sanctioned country be reviewed and authorized in advance by the ECO." Also, the UOV's public website provides information on questions such as when the ECO should be contacted, what does apply for laptops and other electronic devices hand–carried abroad, what classes or courses may be impacted by export controls and also, what is the fundamental research exemption and how should be understood in practice[414].

Second, quite often the university policy on export control emphasizes both the commitment to abide by the applicable laws and the need to respect the academic freedom and the open dissemination of the research results. For example, the University of North Carolina at Pembroke (UNCP) has included an extract from the Faculty Handbook in its export control policy stating: "It is the policy of the University to support and encourage full freedom, within the law, of inquiry, discourse, teaching, research, and publication for all members of this institution's academic staff. The University will not penalize nor discipline members of the faculty because of the exercise of academic freedom in the lawful pursuit of their respective areas of scholarly and professional interest and responsibility." In the same logic, the University of Washington seeks to comply with federal laws and regulations governing

[413] See the website of the UOV: "FIN-043: Managing Exports of Controlled Technology to Foreign Persons and Destinations in Support of Research and Scholars," available in: hipttp://uvapolicy.virginia.edu/policy/FIN-043.

[414] For further information consult the website of UOV dedicated to export compliance and the section of frequently asked questions, available in: http://export.virginia.edu/.

exports and ensure that such compliance is consistent with the University's open academic environment[415].

Third, in the US university setting, primary responsibility for export compliance rests with the lead researchers for grants or contracts –known usually as Principal Investigators (PIs) - who shall be in position to identify risks and inform personnel involved in their research for such risks. Also, there must be an Export Control Office raising awareness and assisting the PIs in their responsibilities. Reviewing collaboration agreements and contracts, determining whether a technology to be used in connection with a research project is controlled, performing risk assessment and record keeping procedures are among the responsibilities of such an office. It might be the case that this role is entrusted to the Office of Sponsored Research or the University legal service depending on the structure of the university in examination. In any case, an institutional official will be in charge of the overall coordination and implementation of the compliance system and certainly legal expertise is *sine qua non* for the operation of such a system. Also, a mechanism for reporting and verifying possible violations is normally in place. For documented or validated violations escalation procedures may be foreseen. Investigations of export control issues demand review at senior level (*e.g.* Provost/Vice Chancellor for Academic Affairs) as it is the case for the policy statements committing universities to abide by the export control regulations.

Fourth, the definition and applicability of the Fundamental Research Exemption (FRE) is an issue of central importance in related policies and information made available in the university websites. The criterion used invariably for deciding whether scientific and technical information resulting from a project or activity qualifies for the FRE is the absence of restrictions on publication or other restriction on the dissemination of such information on the part of sponsors[416]. For instance, the Harvard T.H. Chan School of Public Health clarifies in its export control website that the FRE does not apply with regards to transmissions of material goods. It also points the cases where the FRE is 'destroyed'[417]. If the university accepts any contract clause that forbids the participation of foreign persons, that gives the sponsor a right to approve publications resulting from the research, or otherwise, operates to restrict participation in research and/or access to and disclosure of research results, the FRE ceases to apply. In fact, most universities provide extensive guidance including examples and practical advice to their researchers for taking advantage of the FRE. As the UNCP export control policy sets, it is to the benefit of the university to pursue its mission in a manner that is consistent with all applicable regulations while making reasonable efforts to maximize opportunities where the FRE can be claimed. Negotiating with research sponsors the removal

[415] See the policy statement in the UW website available in: https://www.washington.edu/research/?page=ecr.
[416] See for instance the guidance provided on the Oregon State University, University of California (Berkeley) and Massachusetts Institute of Technology websites, available in: http://research.oregonstate.edu/export/fundamental-research-exemption; http://www.spo.berkeley.edu/policy/exportcontrol.html; http://osp.mit.edu/compliance/export-controls/research/fundamental-research.
[417] Information drawn from the Harvard T.H. Chan School of Public Health website, available in: http://www.hsph.harvard.edu/export-controls/fundamental-research/.

or modification of contract provisions and publishing research papers prior to attending a conference abroad are such ways suggested by many US universities for invoking the FRE.

To conclude, the investigation in the websites of different US universities confirmed that a great number of them have established export control policies and procedures including specific guidance and special websites dedicated to compliance with export controls and sanctions law. It would not be an exaggeration to say that information published in such websites provides a good insight into the US export control legislation as well as the ways that the latter is interpreted and implemented in a research context. Of course, different universities may publish more or less detailed information, adopt most or least elaborate procedures and invest resources according to their core competences and needs.

7.2.2 An Insight into university practices in the EU

The study relied on two sources of information for verifying the state of play with regards to university export compliance in the EU, namely web-based research and direct inquiries to academics working for different European universities. In relation to the latter, an inquiry was addressed to a total of 160 professors and senior academics being involved in the evaluation of research proposals under the H2020. After a brief introduction to the main objectives of dual-use trade controls and the role of the EU regulation, the academics were called to answer whether:

I. they are aware of dual-use issues and the requirements set in the EU regulation
II. they know what is the state of play (awareness, compliance) with regards to such issues in their respective institutions
III. there is somebody in their institution taking care of possible export control issues

The ultimate aim was to verify the level of awareness in different EU universities, contact those employees or departments in charge of export compliance and explore further sources of information in their university websites. The published 'lists of experts' containing the names of the external evaluators of research proposals in the framework of H2020 were utilised for selecting a suitable sample[418]. The sample is made up of academics representing mainly applied sciences and coming from a variety of EU countries. The selected experts participate in the evaluation of proposals falling mainly under the specific area of H2020 'industrial leadership' and concerning research disciplines such as nanotechnology, advanced materials, biotechnology, advanced manufacturing and processing, and space. A total of 28 replies were collected representing universities from Austria, Belgium, Denmark, France, Germany, Hungary, Italy, Poland, Portugal, Spain, Sweden and the UK. Although the response rate does not permit to draw safe inferences for the overall situation in the EU, the findings are indicative of practices followed and problems arising in the EU context. The evaluation of the results can be found in the following section.

[418] The lists are available by DG Research and Innovation in the Participants' Portal under the section Reference Documents, retrieved from: http://ec.europa.eu/research/participants/portal/desktop/en/funding/reference_docs.html#h2020-expertslists-excellent-erc.

The Findings of the Survey: Half of the academics replied that they do not know about the issues in question. The rest replied that they are partly aware of the dual-use concept and linked problems. In fact, 25% of the academics are aware of the dual-use regulation in particular whereas only 14% of their respective institutions implement a sort of compliance mechanism such as ethics committees on dual-use research and provision of related information on the universities' websites.

First, the level of awareness of dual-use issues among the evaluators of H2020 proposals does not appear to be high. This does not imply necessarily a flaw in the evaluation process since only some of the evaluators are also in charge of the ethics screening. The rest are concerned with other aspects such as the evaluation of scientific and technical parameters of the proposals. Quite interestingly, two of the respondents provided more specific information on their role as ethical reviewers. Both of them acknowledged that the dual-use regulation is one of the instruments used in the evaluation of proposals. "Checking the potential risks of research proposals involving transnational cooperation and technologies of dual-use concern are among the tasks entrusted to the reviewers," the first evaluator said. The other evaluator stressed that in all evaluations he was involved there was no concrete dual-use concern. Several reasons are likely to have contributed to this fact. To quote his words, "maybe, the most important is that the call topics I was involved were mostly at a very early stage of the innovation chain, not being fundamental research, but always at quite Low Technology Readiness Levels (TRL)". He also pointed out that "although it is clear that in most cases future innovation branches may also include non-peaceful applications, the calls and also the principles of H2020 agenda make clear that civil purposes are targeted". As a result "the proposals really focus on civil applications when discussing the potential impact and innovation of research". Exploring the potential of a research project to contribute to non-peaceful applications is a useful action to take from an early stage. However, determining whether there is a high probability of an export control risk to materialise is particularly challenging given that the evaluators are not export control trained and the applicable legislation is not always clear-cut.

A remark concerning the role of TRLs is pertinent here. Generally speaking, the TRLs are a nine-step scale for assessing the readiness of a given technology to be used for practical purposes. The TRLs metric was first developed by NASA scientists in 1970s and adopted by the Air Force Research Laboratory as a means of evaluating the readiness of technologies to be incorporated into a weapon or other type of system[419]. In fact, there are several –slightly varying- TRL scales used by governments and managers to select mature technologies for

[419] The amended TRL scale used by the National Aeronautics and Space Administration (NASA) can be found in the following link:
https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html;
See also: Ricardo Valerdi and Ron J. Kohl, "An Approach to Technology Risk Management", paper prepared for the Engineering Systems Division Symposium, MIT, Cambridge, MA, March 29-31, 2004, 2.

inclusion in their programs. The 'Build in Canada Innovation Program' is such an example of a public funding scheme using the TRLs metric[420].

Table VII: TRLs according to the Work Programme 2014-2015 of H2020[421]

Technology Readiness Levels according to H2020 rules	
TRL-1	Basic Principles Observed
TRL-2	Technology Concept Formulated
TRL-3	Experimental Proof of Concept
TRL-4	Technology Validated in Lab
TRL-5	Technology Validated in Relevant Environment (industrially relevant environment in the case of key enabling technologies)
TRL-6	Technology Demonstrated in Relevant Environment (industrially relevant environment in the case of key enabling technologies)
TRL-7	System Prototype Demonstration in Operational Environment
TRL-8	System Complete and Qualified
TRL-9	Actual System Proven in Operational Environment (competitive manufacturing in the case of key enabling technologies; or in space)

In practice, the TRL scale ranges from the idea (level 1) to the full deployment of the product in the marketplace (level 9). More specifically, the first level is the lowest one and concerns 'basic research' relating to a technical field (*e.g.* fundamental investigations and related studies). The second level concerns applied research such as analytical studies and experimentation for formulating a technology concept and/or applications. In the H2020 context, wherever a call for proposals refers to or requires a specific TRL, the TRL scale specified in the General Annexes to the H2020 Work Program must be used. According to the evaluator, the TRLs are utilised also as a means for assessing whether dual-use risks connect to a specific proposal.

Second, it is rather worrying that half of the respondents seem to be unaware of the dual-use concept in general and export controls in particular. Certainly, it is not each and every researcher or university concerned with export controls but justifiably, one cannot be responsible if he or she is not aware of the existence of a problem. In some cases, the

[420] More information on the BCIP can be found here: https://buyandsell.gc.ca/initiatives-and-programs/build-in-canada-innovation-program-bcip/program-specifics/technology-readiness-levels.
[421] See the H2020 Work Programme 2014-2015, *General Annexes*, 29, retrieved from: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-ga_en.pdf.

responses were quite unexpected. Academics dealing with nanotechnologies or conducting research in electric propulsion replied 'we are not concerned' or even 'we do not know about the issues in question' or, 'we do not do nuclear research'. Moreover, it was revealed that scientists working for institutions known to implement export compliance measures, they might be still unaware of dual-use issues. Being responsible in the conduct of research is also a matter of personal consciousness but such findings may indicate a need to step up awareness raising activities undertaken by both academic institutions and regulatory authorities.

Third, the survey shows that quite often universities address dual-use issues in the framework of ethics committees and codes of scientific conduct. Generally speaking, universities may adopt codes of ethical conduct covering from scientific fraud and ethical conduct of research to issues such as conflicts of interest and corruption[422]. Especially for life science research involving for instance, clinical trials and animals testing further guidance and universal codes of conduct are provided by international organisations, university networks and national academies of science[423]. The survey also suggests that the establishment of some kind of ethics committee or advisory body overseeing the implementation of such codes of conduct or other regulations and guidelines is a quite common practice in a research context. In Portugal, the University of Coimbra (UC) has established an ethical commission in charge of the screening of proposed projects requiring clinical trials[424]. However, till now dual-use has never been an issue for research and studies carried out in the Faculty of Pharmacy of UC.

In Belgium, the University of Leuven (KUL) has set up separate committees in charge of different aspects of research such as medical ethics, social and societal ethics, laboratory experimentation, data privacy, scientific integrity and most interestingly dual-use research[425]. KUL researchers rely on existing mechanisms for getting approval for certain types of research, reporting claims concerning current or past incidents or asking advice. In practice, the University offers a flowchart to advise researchers when they need to contact the different committees in place (see the Annex at the end of the study).

The public website of the Ethics Committee on Dual-Use Research (EC DU) draws from definitions and information used in the H2020 sources for discussing dual-use research. Therefore, one could assume that awareness of export control issues is owed partly to

[422] One example is the Code of Conduct governing research in the University of Roma 'Tor Vergata' available in:
http://web.uniroma2.it/modules.php?name=Content&action=showattach&attach_id=13032.
[423] Indicatively one could consult the following:
WHO, *Responsible Life Sciences Research for Global Health Security, A Guidance Document*, 2010, Geneva, retrieved from:
http://apps.who.int/iris/bitstream/10665/70507/1/WHO_HSE_GAR_BDP_2010.2_eng.pdf.
Royal Netherlands Academy of Arts and Sciences, *Improving Biosecurity, Assessment of Dual-use Research*, 2013, retrieved from: https://www.knaw.nl/shared/resources/actueel/publicaties/pdf/advies-biosecurity-engels-web.
[424] The webpage of the ethics commission can be consulted in the following link:
http://www.uc.pt/fmuc/orgaosconsultivos/comissaoetica.
[425] The relevant information can be found in the KUL website, available in:
https://www.kuleuven.be/english/research/integrity/committees.

initiatives undertaken under the Horizon 2020 and explained in chapter 4.1. An application form for requesting approval by the dual-use committee is also available in its public website[426]. The applicants are called to provide a short description of the project that is already submitted or about to be submitted for funding including also the sponsor's description. For research involving cross border transfers, researchers are required to declare how they conform to the imperatives set by the dual-use regulation. Researchers must also clarify whether their research is subject to 'military ethical standards' or otherwise, has potentially military applications. In that regard, pathogen-related research, autonomous robotics, drones and specific laser technologies are mentioned as examples of potentially sensitive research. In case of research funded by military organisations further information is required. Depending on the source of the funding the assessment of the committee may have either an advisory or a binding character. For instance, for projects funded under the H2020 and relating EU funding schemes the final approval rests on the EU funding body. Instead, for research funded through internal and federal funds the opinion of committee will be binding.

The University of Uppsala in Sweden constitutes another example of academic institution addressing export controls in the context of the broader ethics discussion. The CODEX website run by the Swedish Research Council in collaboration with the university's centre for Research Ethics and Bioethics addresses different types of concern relating to broad areas of science[427]. Dual use research is mentioned in connection with natural sciences. The website offers an overview of the legislation including links to non-proliferation Treaties and the UNSCR 1540, national laws administered by the Swedish Agency for Non-Proliferation and Export Controls, the EU regulation and sanction regulations. While the website provides a good insight into the logic and main issues relating to export controls, it is highly probable that no formal procedure or mechanism addressing export control concerns exists. It comes out that it is the sole responsibility of the researcher to identify such an issue and ask for an authorisation as required by the law.

Fourth, there must be a relationship between proactive university compliance stance and vigorous implementation of trade controls involving for instance in-reach activities towards the academia by the regulatory authorities. For instance, universities established in Members States known to dedicate increased resources to export controls such as Germany and the UK appear to be in general better informed compared to universities originating from other Member States. The validity of this argument requires further evidence and it does not imply an inadequate implementation of export controls by other Member States. For example, the survey showed that universities based in Member States such as Belgium, Portugal and Sweden can be aware of export controls as well.

Another interesting remark is that even in cases where the evaluators were aware of the dual-use problematic and stated with most or least certainty that their respective institutions take

[426] The form can be accessed in the following link: http://www.kuleuven.be/ethicsatarenberg/page.php?FILE=subject&ID=676&PAGE=1&LAN=E.
[427] University of Uppsala website, "CODEX: rules and guidelines for research: Dual-use research" retrieved from: http://www.codex.vr.se/en/teknat4.shtml.

care of such issues further inquiries to the Universities were most of the time unsuccessful. Additionally, certain responses in the survey and further contacts with university officers suggest that the EU universities have become aware of export control issues only recently. In addition, for certain universities it is clear that specific policies addressing such concerns will not be introduced. In the words of a legal officer, "we are unlikely to have a large number of projects concerned by dual-use requirements and therefore, we would intend to consider them on a case-by-case basis rather than put in place an explicit policy or process".

The UK's Approach by Alpha Project: With a view to completing the analysis of the situation in the EU a special reference must be done to the situation in the UK. The Higher Education Guide and Toolkit on Export Controls drafted by the Project Alpha of the King's College of London (KCL) and the Association of University Legal Practitioners constitutes a good basis for discussing different aspects of the UK system[428]. The document was prepared with support from the UK's Export Control Organisation (ECO) and offers an analysis of the UK legislation affecting potentially the activities of academic institutions. Also, it provides advice and specific tools such as fictitious case studies, flowcharts, models of policy statements and examples of 'red flags' for addressing export control issues and complying with the applicable laws in a university setting. This is probably one of the very few initiatives taken with the support of an export control authority in the EU and providing detailed guidance to academic institutions[429].

Three remarks are relevant here. First, the document provides an insight into the approach of the UK authorities concerning all different aspects of export controls. What does the term 'export' comprise according to the UK interpretation? What might be considered as technology 'necessary' for the development, production and use of a controlled item? The Guide discusses also the decontrols for information 'in the public domain' and 'basic research' on the basis of the Export Control Order of 2008. Whereas both the UK legislation and the Guide do not go too far in relation to what is already known by the EU regulation, certain issues are clarified. For instance, item, information, technology or research is not in the public domain if [430]:

- needs to be bought from a supplier who controls the supply;
- requires registration;
- is restricted for access by certain people only; or

[428] The Higher Education Guide and Toolkit on Export Controls and the ATAS Student Vetting Scheme, drafted in partnership by the Association of University Legal Practitioners and Project Alpha of King's College London and with support of Export Control Organisation and the Foreign and Commonwealth Office, (April 2015) can be consulted in: http://www.projectalpha.eu/academia.
[429] In addition to the guide be the Alpha project, the British licensing authority has published specific guidance on the topic: UK Department of Business, Innovation and Skill (BIS), Export Control Organisation, *Guidance on Export Control Legislation for Academics and Researchers in the UK*, 2010, available in: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/68680/Guidance_on_Export_Control_Legislation_for_academics_and_researchers_in_the_UK.pdf
[430] The Higher Education Guide, 17.

- is subject to Government and Ministry of Defence security classifications (e.g. commercially confidential information, Official Secrets Act, etc.).

Second, it is clarified that the public domain and basic research exemptions do not apply in the case of an end-use or sanctions control[431]. It could be interesting to know if such an interpretation is shared by all EU Member States. Different Member States have acknowledged that applying catch-all controls in the context of research activities involving transfers of items and technologies is a plausible case[432]. However, it is not clear whether the implementation of a catch-all control impairs the applicability of decontrols. This could potentially mean the unlimited discretion of a licensing authority to decide on the dissemination of any scientific information or technology. In response to this, section 8 §1 of the UK Export Act (2002) stipulates that any interference of protected freedoms must be no more than is strictly necessary[433].

It should be also reminded that end-use controls are implemented on the condition that the exporter has been informed by the competent authority or he is aware that an item, technology, software or service is to be used in connection with a WMD purpose outside the EU. In the UK practice, transfers of technology and software also within the UK are included in the scope of end-use controls where the transferor knows or has been informed that the technology is intended to be used outside the EU for such a purpose[434]. This means that for example, teaching in the context of a university course may fall within the purview of an end-use control.

Third, another means for addressing proliferation concerns in the UK context is the Academic Technology Approval Scheme (ATAS) operated by the Foreign and Commonwealth Office. The ATAS is a student vetting scheme for nationals who originate from countries other than the UK, EEA, or Switzerland and wish to study in a British university[435]. In practice, ATAS certificate seeks to ensure that individuals who apply to study certain sensitive subjects do not have links to WMD programmes. ATAS certificates are required in addition to the normal visa procedures for certain post-graduate courses. It is the responsibility of the University to assign the appropriate Joint Academic Coding System (JACS) code and inform the applicant students if an ATAS requirement applies for their course program.

It should be noted that in the EU, non-proliferation concerns are dealt with in the framework of student visa procedures. For short stays -up to three months- the common visa procedures

[431] Certain provision of Articles 6, 7, 10, 11, 12 and 19 of the Export Control Order supplement the catch-all provision of the Regulation by clarifying the specific cases where a transfer or export of non-listed items, software, technology or service may require an authorisation. See the Export Control Order 2008, retrieved from: http://www.legislation.gov.uk/uksi/2008/3231/pdfs/uksi_20083231_en.pdf.

[432] This was for instance the opinion of the Member States that participated at the 7th ESARDA Export Control Working Group.

[433] UK Export Control Act 2002, 5-6, available in: http://www.legislation.gov.uk/ukpga/2002/28/pdfs/ukpga_20020028_en.pdf.

[434] See Article 10 of the Export Control Order 2008.

[435] For more information on ATAS see the webpage of the UK government: https://www.gov.uk/guidance/academic-technology-approval-scheme.

for the Schengen Area apply[436]. However, for longer stays, applicants are required to follow the procedures set at national level (normally a resident permit will also be required in addition to a valid visa). In practical terms, the extent to which a non-proliferation screening takes place may vary from country to country. For instance, certain Member States appear to be quite proactive by proceeding to inter-service consultations between visa issuing authorities (such as consulates and embassies) and other security agencies -including export control authorities- prior to approving visa applications[437].

Examples of University Compliance Practices in the UK: It is useful to take a look at the ways whereby UK universities respond in practice to requirements set in the legislation. The section draws mainly on information available in the websites of renowned British universities undertaking multidisciplinary research and promoting innovation through partnerships with industry and other research organisations[438]. First of all, as it was shown also in the survey, ethics committees and policies for research integrity are in place. This is particularly the case for research involving humans and clinical trials with human tissue or, using personal data of individuals[439]. For instance, the Cambridge University has four School-level Research Ethics Committees and in addition, some departments, faculties and institutes also have their own local committees. In relation to this, funding organisations such as the Economic and Social Research Council (ESRC) may require from universities to have some sort of internal mechanism for ethical review of all research funded under their frameworks.

> We believe that deciding what to research is a matter for the individual researcher or research group. This belief reflects the value we accord to the principle of academic freedom, enabling the pursuit of academic enquiry subject to the norms and standards of scholarly undertaking, without interference or penalty. This freedom […] will ensure that our strong core disciplines flourish.
>
> *Oxford Research Strategy*[440]

Export Controls are among the issues addressed by the main research policies on approval procedures for sponsored research and collaboration agreements with third organisations. For instance, the webpage of the Imperial College London has a specific section with the heading 'non-standard factors' that can affect the normal application process or contract negotiation

[436] For more information on the Schengen Area visa policies see the website of DG Home: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm.
[437] Information drawn from discussions with Member State representatives in the margins of the 55th Dual-Use Coordination Group meeting, 24 September, 2015.
[438] The websites of the University of Cambridge, University of Oxford and the Imperial College of London were used as a source of information.
[439] See for instance the webpages of the Imperial College London Research Ethics Committee: http://www.imperial.ac.uk/research-ethics-committee/purpose-of-icrec/; the University of Cambridge Research Ethics webpage http://www.research-integrity.admin.cam.ac.uk/research-ethics and the Central University Research Ethics Committee (CUREC) of the Oxford University: https://www.admin.ox.ac.uk/curec/.
[440] Information retrieved from the website of the Oxford University, available in: https://www.ox.ac.uk/about/organisation/strategic-plan/research?wssl=1.

and, which may delay the Institutional Authorisation to submit the application or execute the agreement, if not established and considered in the early stages of proposal development. Among these factors is 'research that can be used or modified for military purposes'[441]. In addition, the Research Office provides further guidance on the issue of export controls. This is the case also with other Universities such as Cambridge and Oxford.

In practice, the Universities under examination offer basic information on the legislation, examples of controlled items, and make special references to end-use controls. The Oxford for instance, clarifies that the research service has registered on the University's behalf in SPIRE so that licence applications and queries can be submitted and that, individual researchers can also directly register on SPIRE[442]. In addition, the university websites provide links to the consolidated UK control list of dual-use and military items as well as the guidance provided by the UK government and the Higher Education Guide.

Export control issues are dealt with mainly by officers from the legal or technology transfer departments and staff from research offices. Contacts with officers from the legal and research services confirmed that presently there are not comprehensive policies and internal controls on export compliance. As R. Boyle notes "in Cambridge responsibility lies primarily within departments and with researchers, partly because Cambridge is quite decentralised and also because the export control regime is very technical -only the actual researchers may know if their experiments might be captured by the controls". Some universities such as the Imperial College of London operate central research compliance offices dealing with legal, ethical and scientific aspects in certain areas of research such as healthcare. It is worth wondering whether existing mechanisms such as central research offices could assume a more proactive role in ensuring compliance with export controls. In any case, raising awareness through websites and information seminars for scientific and administrative staff as well as providing points of contact for export control queries are among the initiatives increasingly taken by many British universities[443].

[441] See relevant information in: http://www.imperial.ac.uk/research-and-innovation/research-office/preparing-a-proposal/non-standard-factors/.
[442]Information retrieved from the University of Oxford webpage offering "Guidance on Export Control Legislation", available in: https://www.admin.ox.ac.uk/researchsupport/contracts/export/.
[443] See indicatively, information provided by the University of Birmingham: https://intranet.birmingham.ac.uk/as/registry/policy/programmemodule/programmes/exportcontrols.aspx and, the export controls policy of the University of Surrey in: http://www.surrey.ac.uk/policies/export_controls_policy.htm.

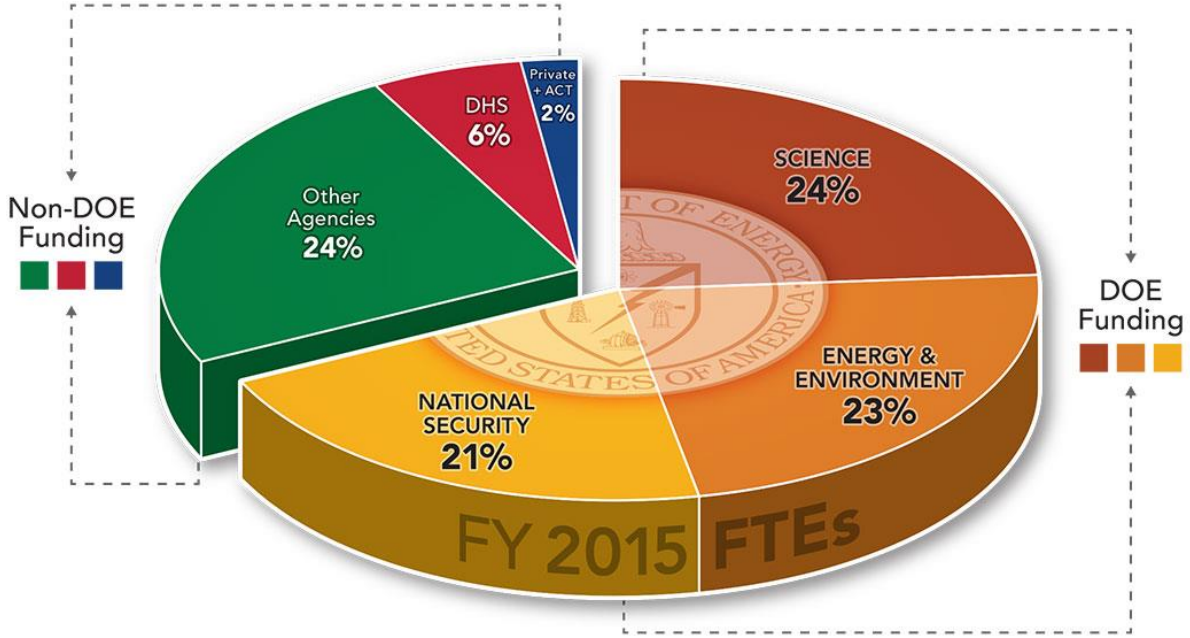
7.3 Other research organisations

This section analyses the cases of two non-university research organisations in the US and Germany with a view to elucidating what are the export compliance strategies adopted and practices implemented pursuant to export control laws.

7.3.1 The Pacific Northwest National Laboratory (PNNL)

The Identity of the Organisation: The PNNL was founded in 1965 and is operated since then by Battelle the world's largest non-profit R&D organization[444]. It is one of the 10 U.S. Department of Energy national laboratories managed by DOE's Office of Science[445]. It conducts innovative research in a variety of disciplines from environmental molecular sciences and biotechnology to security including cyber security and non-proliferation matters. PNNL operates research facilities in different locations in the US territory such as in Washington and Oregon and its main campus is located in Richland (Washington). It undertakes research for and collaborates with government agencies, universities and industry. Its R&D expenditure for fiscal year 2015 was $955 million and made up of funding sources including the DOE, other federal, State and local agencies, universities and industry sponsors. Around 4.300 scientists, engineers and non-technical staff are employed in its premises and the number of visiting scientists and other users was 2000 for 2013.

Figure XII: Sources of R&D expenditure for fiscal year 2015[446]



[444] Battelle headquartered in Columbus (Ohio) has managed and operated PNNL for DOE and its predecessors since the Laboratory's inception in 1965.
[445] There is a total of 17 National Laboratories managed for the account of DOE. The Office of Science is the steward for 10 of them. More information can be found on the website of the US DOE, Office of Science, available in: http://science.energy.gov/laboratories/.
[446] PNNL website: About PNNL Business Facts, Fiscal Year 2014, retrieved from: http://www.pnnl.gov/about/facts.asp.

Export Compliance Practice at PNNL[447]: The PNNL Export Control Office (ECO) was formally set up in 2009 with the task of reviewing all the activities of the organisation requiring an export control clearance. The realisation of the importance of operating an internal export compliance system originated from contacts and communications with the competent regulatory authority. With regards to organisational and operational aspects, the ECO employs currently 4 fulltime staff members including the manager and receives support from at least 8 other employees from the legal, property, contracts and procurement departments. PNNL's compliance office resides in the Safeguards and Security Services Division (SSSD) and it represents a stand-alone function. The overall responsibility for export compliance lies with the legal department whereas the day-to-day supervision of export related tasks is assumed by the ECO manager. It is estimated that the full development and operation of the compliance policies and procedures took about two to three years from the moment of the initial inception of the system. This seems to be in accordance with what section 7.2.1 suggests for the US universities.

The PNNL's capabilities cover different points in the spectrum of scientific activities from basic to applied research and export controls do affect its collaboration with industry and academia (joint projects, licensing invention/patents and consulting services). In fact, the PNNL has applied for different types of authorisations pursuant to military, dual-use, nuclear and sanction controls. Concerning risk management practices, a useful way for assessing the risks and identifying priority areas is at the phase of planning of a new research project. Many companies operate a 'Gate Review Process' that is a conceptual and operational road map for moving a new project from idea to launch. Researchers getting engaged in such a process need to contact the security, legal and export control services prior to entering into a formal collaboration with an industry partner. This way potential export control risks are assessed at an early stage.

A. Rittel, export compliance manager at PNNL considers that making the staff aware of export compliance and training them on the occasions requiring contacting the ECO for further advice is a key element for the proper functioning of the system. In relation to this, particular attention has been paid to training activities. The ECO conducts routinely training seminars upon request by the lab personnel and whenever is deemed as necessary. Export control modules and objectives have been incorporated into the annual security refresher -an electronic awareness raising course- and general awareness brochures dealing with a range of compliance matters. In addition, an export control website available internally and a video series freely accessible in the 'YouTube' can be consulted for drawing further information on export controls. On top of that, commitment statements by lab directors and videos having as spokespersons officers high in rank increase the consciousness that export compliance does matter for the organisation.

When it comes to technology controls a variety of tools are utilised for monitoring sensitive transfers. Security clearances for hiring new staff, approval procedures for foreign visitors and travels abroad as well as access controls, and specific procedures for IT security are all

[447] Information retrieved after communication with Alan Rittel, export control manager at PNNL.

included in the quiver of the export compliance strategy. The implementation of export compliance measures is underpinned by policies and accompanying material such as an export control manual for lab personnel and an export guidebook for export control staff. Although a lab procedure exclusive to export compliance does not exist, export control requirements are embedded in the major activities in which PNNL is involved such as international shipping and foreign national visits. Not surprisingly, the implementation of the deemed export rule represents a quite challenging issue in a research organisation employing several foreign scientists for accomplishing its research portfolio. The application of the fundamental research exclusion is done on the basis of the intent to publish the results of a scientific research. Also, it requires assessing any security implications of a given publication and the close collaboration between the export control officers and the researchers.

The PNNL is working to set a higher standard in export compliance and non-proliferation by considering all available means. It also recognizes that it must increase visibility of PNNL's export control compliance program and step up compliance efforts in certain respects. For instance, implementing stringent compliance practices such as preferentially procuring from and subcontracting with companies that maintain strong export compliance programs and, considering inclusion of export control objectives in key management documents are such initiatives under consideration[448]. Although the US authorities have not published best practices and specific standards for national laboratories, quite similar approaches are implemented across the DOE lab complex. In relation to this, there is also the Office of Safety and Security Policy operated by DOE and overseeing the safety and security policies and procedures implemented by different national laboratories. Export control policies are not explicitly mentioned among the areas dealt with by this office[449].

7.3.2 The Helmholtz Zentrum of Berlin (HZB)[450]

The Identity of the Organisation: The 'Helmholtz Zentrum Berlin für Materialien und Energie GmbH' (HZB) is a member of the Helmholtz Association. The latter is made up of 18 centres representing Germany's largest scientific research community with activities throughout Europe and worldwide. Each year, thousand scientists and researchers come to the Helmholtz Centres from all over the world to work on the large-scale scientific facilities and instrumentation that these centres provide. In some cases, this equipment is the only one of its kind in the world. Although legally independent, representatives from federal and Länder government participate in the external decision making body –the senate- coordinating *inter alia* in which areas public money should be allocated. One could reasonably expect that the largest German research association performing cutting-edge reseaech in a variety of areas takes precautions against export control risks. For that case study the spotlight is on HZB.

[448] Information from presentation" by Kevin Whattam, "Enhancing Export Control Awareness at PNNL, at 5th ESARDA Export Control Working Group Meeting, November 11-12, 2014, Rome, Italy.
[449] Information retrieved from the website of Office of Science, DOE, available in: http://science.energy.gov/laboratories/.
[450] Information drawn from the official websites: https://www.helmholtz-berlin.de/zentrum/index_en.html and, http://www.helmholtz.de/en/about_us/die_gemeinschaft/facts_and_figures/.

Table VIII: The Helmholtz Association at a glance

The Helmholtz Association	
N^{o} of research centres:	18 throughout Germany
International offices:	Brussels, Moscow, Beijing
Scope of research activities:	1. Energy, 2.Earth and Environment, 3.Health, 4.Aeronautics, Space and Transport, 5.Key Technologies, 6. Structure of Matter
N^{o} of employees: (2013 figures)	38,036 of which 14,734 are scientists
N^{o} of foreign scientists: (2014 figures)	7,476 work at the Helmholtz Centres
Budget*:(2015 figures)*	€4.24 billion (2/3 from public sponsors)
N^{o} of publications: (2014 figures)	13,549 in ISI or SCOPUS-indexed scientific journals
N^{o} of patents:	An average of 400 patents each year
Revenue from collaborations with industry:	About 2,000 collaborative projects with industry with revenues of appr. €158 million
Revenue from licensing agreements:	€14.2 million from about 1,400 licencing agreements

The main areas of activity of HZB relate to the exploration and test of new materials and complex material systems that help to face challenges such as energy conversion and efficient use of energy and resources in information technology. To that effect, HZB operates two large-scale facilities for basic physics research on the structure and function of matter: the research reactor BER II for neutron experiments and the third generation synchrotron radiation source BESSY II including a number of state-of-the-art laboratories and user facilities. This research infrastructure is used by researchers from universities, foreign research institutions and industry. Indeed, the two HZB campuses -Wannsee and Adlershof-

welcome each year about 3,000 visiting scientists[451]. Although HZB work has exclusively a focus on peaceful applications, the dual-use nature of certain facilities and equipment used and the high number of collaborations and exchanges with foreign scientists and universities may pose some security risks including export related ones. HZB acknowledging this contingency implements a number of safety and security measures including export compliance procedures.

Table IX: The identity of the Helmholtz Centre Berlin (HZB)

The Helmholtz Zentrum Berlin (HZB)	
N^{o} of employees:	1,114
Visiting scientists:(including trainees and PhD students)	3,000
Campuses:	Berlin-Wannsee and Berlin-Adlershof
Budget:	€146 million Euros (2015)
Partners:	About 400 German and international universities, research institutes, and companies

Export Compliance Organisation at HZB[452]: In HZB, export compliance is considered as a stand-alone function and it is coordinated by a legal advisor setting the main policies and procedures to be followed by all staff concerned and, supervising the work of the different employees in charge of export compliance. The legal advisor reports directly, at senior level, to the Administrative Director who bears the overall responsibility for export compliance. Nonetheless, the day-to-day execution of export related tasks is dealt with mainly by staff in the Purchasing and Materials Logistics department. Indeed, the legal advisor and the responsible staff from the Purchasing and Materials Logistics –a total of three people- they are assigned as Export Control Officers (ECOs). As it is the case with other organisations, the ECOs are not solely concerned with export compliance and they collaborate with colleagues from other departments as appropriate. The Legal Office, the Personnel and Social Matters Department and the Compliance Management Office are the most common examples of other services contributing to export compliance objectives. In addition, the User Coordination Department takes into account export control requirements when implementing approval procedures with regards to the access and use of the HZB facilities by external researchers.

[451] For many research questions, it is a huge advantage to be able to study different material samples using both neutrons and synchrotron radiation: By combining these two complementary methods, a more complete picture of matter is obtained.

[452] Information retrieved from interviews with Dr. Ulrike Behrns, assistant to the Administrative Director and legal advisor on export compliance at HZB.

Last but not least, the scientists themselves are called to provide their expertise and clarify possible implications of their research.

How does the management of a research institution become aware of trade control requirements and perceive export control risks is always an interesting question to ask. Not surprisingly, at HZB the issue of trade controls came to the forefront after an audit conducted by the German customs back in 2007. Thence, a rudimentary compliance mechanism was introduced relying mainly on an electronic system for the monitoring and, approval where appropriate, of all transfers of materials and equipment outside Germany. At the time an e-system for approving visits of foreigner scientists was also set in place. However, this preliminary effort was not backed up with formal export control policies setting main principles and procedures to be followed.

Since 2013 a formal compliance system has been established at HZB and the task to enhance internal compliance controls is seen as an ongoing effort. For tangible transfers, the electronic system in place deals with requirements set in the different legal frameworks: transport and safety rules; import regulations and reporting obligations under the Additional Protocol to Safeguards agreements and naturally, export requirements for dual-use equipment and technology[453]. According to ECO, HZB conducts mainly fundamental research and the number of formal applications for exports to non-EU countries is limited. For 2014, a total of 300 exports were reviewed at the HZB from which 60% concerned transfers within the EU and the rest exports to non-EU destinations. Most of the time, the activities of the HZB involve temporary exports (*e.g.* for repairs), transfers of samples and materials and only rarely transfers of listed dual-use equipment. In fact, for 2014 there has been no license for dual exports whereas in 2015 there was just one authorisation. The risk identification and mitigation concerns in-house activities, activities undertaken abroad as well as screening of cooperation agreements with firms and other research institutions. For dubious cases formal inquiries may be submitted to the German licensing authority. In fact, four formal inquiries to BAFA have been recorded in 2014 and two in 2015.

Concerning transfers of technology, HZB implements internal controls for visiting guests and official travels to non-EU countries. Export control risks are assessed mainly through existing procedures. For example, approval procedures for travels abroad have been established. In the near future, an information sheet regarding information sharing and export risks will be introduced in an electronic workflow required for getting approval for travels abroad. In relation to this, a handbook assisting HZB staff to assess potential risks relating to travels in non-EU countries will be introduced as well. As it is the case with many research establishments access of visiting scientists and employees to certain laboratories or buildings is subject to prior approval and access controls. The screening procedures may differ

[453] In practice, researchers are required first to read information about possible applicable export rules. A pop-up window appears in case of transfer to EU countries- and the applicant has to declare whether an export control issue relates to their transfer. The reason for this is Annex IV that concerns only a limited number of particularly sensitive items and for which a different procedure applies. If there is no such issue then they can proceed with the electronic workflow. Otherwise and in case of exports to non-EU countries, the application is subject to further review by the responsible ECO.

depending on the duration of the guests' stay in the institution. Internal controls apply also for accessing data through the intranet. For example, visitors are able to access only the guest network while employees have normally full access to HZB intranet. As discussed above, HZB has in place a user system allowing external researchers to access its facilities. This is for instance the case for beam-time applications (time allocated to researchers for use of a beam of photons from BESSY II source)[454]. The evaluation of applications concerns as much scientific and technical aspects as security (*e.g.* trade control and sanction requirements) and safety issues (*e.g.* radiation protection rules).

Maintaining high standards of compliance requires increasing the level of awareness and cultivating a culture of compliance. With a view to living up to this challenge, HZB relies on its intranet webpage, internal notes and training sessions for communicating export control objectives. The trainings are half-day seminars taking place once a year and their thematic extends to a broad range of matters such as anticorruption, regulations for publicly funded research and other compliance requirements. The implementation of the export compliance system is monitored and the results are reported once a year to the Administrative Director who evaluates the overall progress and decides for further improvements. Depending on the identified areas of concern ad hoc trainings conducted by the German licensing authority may be scheduled. This possibility is offered by BAFA to every research establishment requesting such training. The ECO singled out the need to ensure proper information sharing and raise awareness as a constant challenge given the dynamic context of the organisation (flows of PhD students, trainees and visiting researchers). Also, striking a balance between the freedom of research and export control regulations is a particularly challenging task given the lack of common criteria to interpret the basic research exemption. Integrating export control objectives to existing procedures and offering regular trainings seem to be a key to establishing a sound internal compliance system in a research setting.

[454] The evaluation of applications for beam-time is entrusted to the HZB Scientific Selection Panel and it involves the scientific and technical assessment of the submitted work as well as a risk assessment. Regular access at HZB is free of charge for national and international academic users. Private sector researchers can use the HZB facilities provided that the research is in collaboration with an academic partner from a university or research organization. However, industry users and any users who do not wish to publish their results of HZB experiments in the public domain they need to purchase beam-time. Information retrieved from: https://www.helmholtz-berlin.de/user/beamtime/types-of-beamtime_en.html.