COUNCIL OF THE EUROPEAN UNION

Brussels, 5 December 2005

15290/05

LIMITE

COMER 179
PESC 1103
CONOP 56
ECO 153
UD 150
ATO 122

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject :	Export controls on transfers of software and technology by intangible means

Delegations will find attached a note, agreed by the Working Party on Dual Use Goods at its meeting on 2 December 2005, on the work done so far in the Dual Use Working Party and Article 18 Co-ordinating Group on the application of ITT controls under Council Regulation (EC) No. 1334/2000.

EXPORT CONTROLS ON TRANSFERS OF SOFTWARE AND TECHNOLOGY BY INTANGIBLE MEANS

1. Introduction

This document captures the work done so far in the Dual Use Working Party and Article 18 Coordinating Group on the application of ITT controls under Council Regulation (EC) No. 1334/2000. It is intended as a basis for further work on the development of best practice guidance for the Member States Licensing Authorities and to be of assistance to Member States in this area.

Intangible transfers of sensitive software and technology involve no border controls and no carriers crossing international frontiers. Frequent scenarios include engineers or technicians using the Internet/an intranet, fax or e-mail to transfer sensitive data, as well as researchers making know-how available abroad through international scientific exchange and cooperation.

2. Background

Article 2(b)(iii) of Council Regulation (EC) No. 1334/2000 ("the Regulation") defines export as "transmission of software or technology by electronic media, fax or telephone to a destination outside the Community. This applies to oral transmission of technology by telephone only where the technology is contained in a document the relevant part of which is read out over the telephone, or is described over the telephone in such a way as to achieve substantially the same result." Article 2(c) describes exporter as "any natural or legal person who decides to transmit software or technology by electronic media, fax or telephone to a destination outside the Community."

The Regulation does not control transfers of technology arising through the move of natural persons across borders. This is covered by Joint Action CFSP 401/2000, which is for EU Member States to implement at a national level.

Following the adoption of the Regulation, a number of Council Working Party and Article 18 Co-ordination Group (CG) meetings took place in 2002 and 2003 which were devoted to the implementation of this Article of the Regulation. Among the issues discussed were the following:

- Whether it would be appropriate to amend article 2(b)(iii) (cf DS 31/2001). No consensus was reached. The legal service of the Council and DG TRADE, supported by some Member States, rejected the suggestion to amend the Regulation to include a reference to internet. The Commission stressed that "internet" is a means of communication covered by the wording "electronic media" of article 2(b)(iii) and that one of the main elements to define whether a transfer is concerned by article 2(b)(iii) is its final destination (since article 2(b)(iii) refers to "a destination outside the EU"). Other elements which must equally be taken into account to define if a transfer is an export is to identify if the item is covered by the Regulation (in particular, is the technology in the public domain as defined in the Annex to the Regulation. Is the item listed or unlisted but covered by articles 4 or 5 of the Regulation? The General Technology and the Nuclear Technology Note indicate that controls on technology transfer do not apply to information in the "public domain", to "basic scientific research" or, as regards the GTN, to the minimum necessary information for patent applications. The GTN says also that "controls do not apply to that technology which is the minimum necessary for the installation, operation, maintenance (checking) and repair of those goods which are not controlled or whose export has been authorised").

- The Article 18 CG meetings offered Member States the opportunity to present their practice and discuss concrete cases, including the definition of public domain and the implementation of the Joint Action.

The Commission Services summed up the state of play of discussion in its 2004 September report to the Council and the European Parliament on the implementation of the Regulation.[1]

---

1 "The basic rule contained in the Regulation is that the exportation of items and technologies (including those engendered by new means of communication) is subject to authorisation. The Regulation does not cover transfers that take place through the cross-border movements of natural persons (Article 3(3)) or data in the public domain. Article 19 of the Regulation criminalises individual acts that infringe the basic rule". "When the Council Group and the Article 18 Group looked into the matter of ITT controls, the conclusion was that amending Article 2(b)(iii) was not necessarily the most practical way of ensuring effective controls on intangible transfers in the EU, given that the challenge is to keep up with ever-changing communications technology. Technological innovation has made information easier to disseminate (but has made controls more complicated because there is potentially more to control), but innovation has also made it easier to identify the people using the information (which facilitates controls).
It was noted that in practice the control procedures established at national level had to take account of the constant evolution of communications technology. It seemed unlikely that a company would decide to make technology subject to export controls freely accessible on the market outside the EU via new communications media, since this would run counter not only to industrial and intellectual property law but also to compliance with the dual-use Regulation."
To ensure that controls are effective and proportionate, the national licence-granting authority needs to have close contacts with the companies and exporters concerned to make sure that it understands their needs and that these are reflected as much as possible in their licences. Some Member States have already indicated that some of their general licences also cover intangible technology transfers. The Commission also encouraged the members of the Group to follow the work of the Council's Working Party on issues relating to new technology and "cyber security. The Commission has asked the Member States on many occasions to notify it of what legislation they have adopted to implement Article 2(b) (iii) of the Regulation."

Subsequently Germany organised a meeting open to all Members of the export control regimes, which addressed ITT controls in Berlin in June 2004.

The International export control regimes have started to prepare guidelines on ITT, in particular the MTCR (German proposal) and the Wassenaar Arrangement (US proposal).

The conclusions of the Peer Reviews of Member States' application of the Regulation recommended the adoption of EU guidelines to implement article 2(b)(iii) as the Peer Review revealed that difficulties in implementing this article remained.

3. Scope of ITT controls within the Regulation

A. General issues regarding the scope of controls

(1) General

All the relevant articles of the Regulation apply to intangible transfers of technology. Thus, as regards catch all; article 4 of the Regulation applies to all technology transfers including transfers by intangible means of non controlled items. The same applies as regards criteria to grant/deny export authorisations (article 8) and notifications of denials (article 9), etc. It is understood that intangible means includes transmission by email.

It is understood that researchers can fall into the scope of the definition of "exporter" and therefore that if they transmit controlled technology in their relations with third parties, the Regulation applies. However the situation of researchers and academic centres raises specific questions regarding the application of the Regulation that will need to be addressed at a later stage. Examples of these questions are, among others, possible enhanced compliance through codes of conduct and common EU understanding of the definition of public domain and basic scientific research, the extent to which researchers and academic centres are allowed under national law to publish sensitive research; whether once published such information can be considered to be in the public domain; whether internet publication can be considered an "export" in the sense of the Regulation; and also the fact that such publications would be non-profit operations (although the Regulation does not require that ITT is carried out of non-profit making purposes). There may also be certain enforcement implications that would deserve examination.

In a number of cases there are questions of interpretation of the Regulation that may deserve further clarification, and which might require in some instances amendments to the Regulation.

(2) Oral communications

Although the Regulation does not specifically mention video conferencing and filming technology, they are examples of forms of communications, which could fall under the definition of "transmission of software or technology by electronic media".

Certain electronic equipment other than the telephone also permits forms of oral communication, such as video-conferencing. Where communication by such means is purely oral, the rule that applies to telephone transfers or transmission by electronic media could apply. The sending by electronic means of filmed documents or papers containing controlled technology, including by videophone, would also require an authorisation as would transfers via text messaging.

An issue to further consider is whether to eliminate the reference in the Regulation that phone or similar transmissions are controlled only where the technology is contained in a document the relevant part of it, as oral or e-transfers of controlled technology can take place without resting on any support, which would be a "document".

(3) Intranet. Making technology/ software available on an intranet or within a shared data environment (SDE)

It could be considered whether making controlled technology or software available on a company's or organisation's intranet or SDE – for example to established customers with access rights - could constitute an electronic transfer, and therefore an authorisation would be required according to the Regulation before that technology or software could be accessed by employees of the company, group, or organisation, outside the Community (taking into account that the CGEA covers those transfers for countries listed in Part 3 of Annex II and technologies listed in Annex I minus part 2 of Annex II).

However, the question whether technically "making available" is not equal to "transmission" as provided for in the Regulation is still open, and such an interpretation could have far reaching consequences both for researchers and for industry. Therefore Member States should consider whether the considerations below would be applicable in such cases.

The point at which an authorisation is required depends on the arrangements made for granting access to the intranet.

If material on an intranet were to be fully accessible by members of the company, group, or dedicated collaborative user-group, situated outside the Community from the time when the material was saved to the site, then an authorisation would be needed before the material was saved to the site. If individual permissions were required for employees or other approved users outside the Community before they could access the site, then it would only be necessary to obtain an authorisation before that permission was given.
Similarly if the employee of a company outside the Community accessed controlled technology or software belonging to his or her company electronically while outside the Community, then this would constitute an electronic transfer of that technology or software to the country in which the individual was situated when they accessed the technology or software. An authorisation would be required for any such transfer, even if the employee abroad had no intention of passing the technology or software on to another person abroad.

This is analogous to the position for physical exports, where taking controlled technology outside the Community, even if only for personal use and not for onward transmission while outside the Community requires an authorisation. Unless the activities were covered by the CGEA or a national general authorisation it would be for the company to ensure that the technology or software was not accessible from outside the Community until an individual or global authorisation was issued.

Many of the issues raised in connection with the intranet could equally apply when dealing with transmission over the internet.

(4) Public domain, basic scientific research and minimum content for patent application exemptions

The Regulation makes it clear that technologies in the public domain or basic scientific research and minimum content for patent application are exempted and a definition of what constitutes those terms is provided for in the Regulation under Annex I. However, interpretation of the definition may differ, this has led to many discussions in the CG and in the Berlin seminar as to what constitutes the public domain. When it comes to export, a technology in the public domain is not subject to export authorisations while a technology not in the public domain would need a prior authorisation in order to be exported.

As far as public funded research activities, which may lead to detrimental applications (dual use, e.g. biological weapons), are concerned, some specific measures may be envisaged to limit the accessibility of data from the general public. This approach, however, should be consistent with domestic regulations in the place where the research is carried out and relevant International Regulations and Conventions (such as the ones indicated in the European Union research programmes).

The posting of product details, photographs, diagrams etc to an internet site which is freely available to the public without further restriction and which do not present infringements to controls mentioned in Annex I arguably cannot be considered to be a transfer of technology and so an authorisation would not be required. In general exporters are unlikely for commercial reasons, to place controlled technology onto freely available sites, which can be accessed by customers or indeed competitors without charge.

Given that the precise interpretation of what constitutes “Public Domain” is still being discussed, the position given above may be subject to change or clarification at some future time. EU Member States may in future need to:

- establish a common interpretation of the definition of the public domain;
- decide whether the making available of a publication on the internet would constitute an export.

This would require, inter alia, investigating national legislation, and for publicly funded research, identifying the appropriate organisations which should introduce restrictions for unpublished controlled technology, taking into account the advantages of international access to technology over the risk of it being used for illicit purposes, WMD proliferation or terrorists attacks.

B. Type of Export Authorisation to cover ITT

(1) Export authorisations

All existing types of export authorisations foreseen in the Regulation can be used for ITT (the Community General Export Authorisation (CGEA), national general export authorisations, global and individual authorisations).

(2) Exceptions

As regards "minimum technology", the item is not covered by the Regulation but in the technology notes in its Annex I and in Annex A to this note which reads as follows: "Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) and repair of those goods which are not controlled or whose exports have been authorised. NB This does not release such technology specified in 1E2002e, 1E0002f, 8E002a and 8E 002b". It could however be considered whether when applying for authorisations, exporters will need to consider if the technology transfers could reasonably be considered as "minimum technology". (See GTN, NTN and GSN in Annex A, part 2). An everyday parallel would be the type of manual that is supplied with a television or washing machine. Typically, it would provide operating instructions, some basic specifications (e.g. operating voltage, operating temperature range etc). Generally, handbooks and technical manuals supplied in electronic format intended to support items in the state in which they were exported would not need to be listed as a separate item on the authorisation application form.

There will be occasions where the technology cannot be considered "minimum". This may apply:

- Where there is no equipment being exported – for example, where an export is a one off transfer of technology, or is in support of equipment that was not supplied by the exporter;
- Where the technology is required to support a complete system, but the goods are components of that system;
- Where the technology is a follow on from previous authorisation (e.g. in fulfilment of a long term contract), but is essentially different from the technology that was originally supplied – for example, handbooks or publications relating to equipment that has been upgraded since its original supply.

In these instances the exporter needs to apply for an individual authorisation if other forms of authorisation are not open to them.

(3) Temporary export authorisations

Where a temporary authorisation for ITT is required it should be applied for in the same way as for physical exports although in most cases this is unlikely to be applicable. If technology passes outside a company's control and on to a third party outside the Community, then in reality that would be an export (permanent transfer), even if that technology were brought back to the Community. However, an example might be where a company takes its own equipment outside the Community for trial or exhibition purposes and needs technology to accompany that export to cover possible repair and maintenance.

C. Use of Annex IIIa (Model Form) for global and individual ITT export authorisations

The question to address is whether the current form of Annex IIIa is appropriate for granting ITT authorisations. Among the issues that would need to be addressed are whether changes may need to be introduced, probably after consultation with industry.

There is no "unlimited quantity" option on the model form set out in Annex IIIa of the Regulation. Therefore, if an application covers both physical and electronic transfers, there is no possibility to differentiate between the two types of transfer, so the quantity should cover only the physical transfers.

Also, in the event that an application only covers electronic transfers, the exporter could either not complete the quantity box, as being not applicable, or if a Member State requires the box to be completed, insert a nominal quantity. Finally, when it comes to placing a value on electronic transfers on the model form, the exporter could be advised to make a best judgement on how much the customer is contracted to, or is likely to spend. If, for example, the technology that is to be transferred electronically has already been paid for as part of the contract for previous supplies of goods, a nominal value could be inserted; if transfers are covered by one separate support contract, that would be the value to be inserted; if it was to be paid for as needed on a number of occasions, then previous or similar contracts might enable the exporter to judge how much was likely to be spent by the customer.

D. End–User Documentation and Intangible Transfers

Industry should be able to identify and grant access to end-users. The end-user documentation that accompanies an application for export authorisation for electronic transfers does not need to be essentially different to that used to support an application for physical transfers. It should be part of the discussion between national authorities and the exporter. If transfers are to take place electronically, an electronic address (fax number or e-mail address) at which the transfers will be received should also be required, along with the standard requirement for the name and address of the end-user.

E. Record-keeping Requirements

Article 16 of the Regulation sets rules for record keeping which legally apply to both physical and intangible transfers. Subsequently and in particular taking into account of the specificity of the organisation and the functioning of researchers and academic centres, some clarification could be brought to this article. Exporters do not need to keep associated e-mails which may relate to the transfer but do not add to it. It is sufficient to identify the technology transferred, the dates between which it was transferred, and the identity of the end-user. Electronic transfers may not pass through a company's export manager who would normally arrange for the necessary paperwork, including export authorisations for physical exports.

Thus record keeping and compliance for transfers by intangible means may be less straightforward. However, transfers by electronic means may often form part of a commercial deal, the contents of which will have been agreed in advance. Thus export managers should have had an opportunity, at the time a contract was finalised, to assess what technology would be transferred by intangible means. How a company keeps these records is up to them. The information might, for example, form part of a contract or project plan, or it may be kept on a central spreadsheet.

These records must be kept for a minimum of 3 years and should be produced to the competent authorities of the Member State in which the exporter is established on request.

F. Compliance and Enforcement

Industry compliance is even more important for intangible transfers of software and technology as those shipments cannot be physically monitored by customs.

(a) Role of Member States

In the first instance, Member States need to identify the potential dual use technologies or items listed in Annex I that could be exported by intangible means from their territory, either by natural or legal persons.

Regarding possible unlawful transfers of technology by academics and research centres, the Member States could consider identifying those individuals or those centres that could be at the source of illicit transfers. The compliance and control enforcement suggestions described below may require adaptation if and when applied to such research centres.

Member States could also systematically try to identify suppliers of those items defined above so as to target "potential exporters". Depending on the characteristics of their domestic supply in the dual use area, Member States could eventually start with major potential exporters of software and technology by intangible means, ensure they are made aware of the controls and procedures for applying for a licence and the penalties for non-compliance.

(b) Compliance

Although some of these questions are currently under review in the context of the Impact Assessment Study (conditioning global authorisation to ICP), some considerations can be considered of relevance already at this stage.

Companies could be encouraged by Member States to have systems in place (internal compliance programme (ICP)) to make sure that all the appropriate staff are 'trained' for example a new employee and 'refresher training' for longer standing members of staff. The company needs to have clearly defined lines of responsibility on export controls, preferably written down and reflected in a formal quality regime. They will also need to possess knowledge of the licensable technology or software and of the related goods that they are exporting or transferring (ideally written down).

These procedures need to be in place to ensure that those transfers or exports of technology or software which require an authorisation are covered by one, and that the person who is transferring or exporting the items knows and can ensure compliance with the authorisation and its conditions.

Industry needs to be prepared to receive compliance checks. They need to know that their records of intangible transfers will be inspected and will include transfers made by individual, global and general authorisations (including the CGEA).

(c) Enforcement

Among possible enforcement measures that can be adopted are compliance visits by national authorities, auditing companies and institutions, post-transfer monitoring by national authorities, and awareness-raising activities. An illustration of such measures is provided in Annex B, although they are not specific to ITT controls.

Annex A

1. Definitions in respect of Technology and Software in Annex I to the Regulation

"Technology" means specific information necessary for the "development", "production" or "use" of goods. This information takes the form of 'technical data' or 'technical assistance'

> ***N.B.1***: 'Technical assistance' may take forms such as instructions, skills, training, working knowledge and consulting services and may involve the transfer of "technical data".
> ***N.B.2***: 'Technical data' may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

"Software" means a collection of one or more 'programmes' or 'micro programmes' fixed in any tangible medium or expression.

> ***N.B.*** 'Micro programme' means a sequence of elementary instructions, maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction into an instruction register.

"Source code" (or source language) is a convenient expression of one or more processes which may be turned by a programming system into equipment executable form.

The associated definitions of "development", "production" and "use" are as follows:

"Development" means all phases prior to "production" such as design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, ("goods" or "software"), configuration design, integration design, layouts;

"Production" means all production phases, such as: construction, product engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

"Use" means operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.

"In the public domain" (GTN, NTN, GSN), as it applies herein, means "technology" or "software" which has been made available without restrictions upon its further dissemination (copyright restrictions do not remove "technology" or "software" from being "in the public domain").

"Basic scientific research" (GTN NTN) means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

"Required" (GTN) as applied to "technology" or "software", refers to only that portion of "technology" or "software" which is peculiarly responsible for achieving or extending the controlled performance levels, characteristics or functions. Such "required" "technology" or "software" may be shared by different goods.

2. Technology and Software Notes in Annex I of the Regulation

(a) Nuclear Technology Note (NTN) - (to be read in conjunction with Section E of Category 0)

The "technology" directly associated with any goods controlled in Category 0 is controlled according to the provisions of Category 0. "Technology" for the "development", "production" or "use" of goods under control remains under control even when applicable to non-controlled goods. The approval of goods for export authorizes the export to the same end-user of the minimum "technology" required for the installation, operation, maintenance and repair of the goods. Controls on "technology" transfer do not apply to information "in the public domain" or to "basic scientific research".

(b) General Technology Note (GTN) - (To be read in conjunction with section E of Categories 1 to 9).

The export of "technology" which is "required" for the "development", "production" or "use" of goods controlled in Categories 1 to 9, is controlled according to the provisions of Categories 1 to 9.

"Technology" "required" for the "development", "production" or "use" of goods under control remains under control even when applicable to non-controlled goods.

Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) and repair of those goods which are not controlled or whose export has been authorised.

NB: This does not release such "technology" specified in 1E002e, 1E002F, 8E002a and 8E002b.

Controls on "technology" transfers do not apply to information "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications.

(c) General Software Note (GSN) - (this note overrides any control within Section D of Categories 0 to 9)

Categories 0 to 9 do not control "software" which is either:

(a) Generally available to the public by being:

1. Sold from stock at retail selling points, without restriction by means of over the counter transactions, mail order transactions, electronic transactions or telephone order transactions and

2. Designed for installation by the end user without further substantial support by the supplier; or

NB: Entry (a) of the GSN does not release "software" specified in Category 5 Part 2 ("Information Security")

(b) "In the public domain".

Annex B

Illustrative description of certain possible enforcement measures

Enforcement of controls on sensitive software and technology should not be limited to certain means of transfer.

Due to the nature of intangible transfers of software and technology, border controls by customs authorities are not possible. Customs and other investigation authorities can, however, conduct audits of companies and institutions to ensure compliance with export control and in some Member States.

Enforcement of controls on the transfer of software and technology by intangible means poses a different set of problems and challenges to those faced when enforcing physical transfers. While specialist techniques are available to monitor communications traffic[1] and investigate breaches it is nevertheless far more difficult to prevent actual transfers taking place, if that transfer is made by intangible means. Such transfers therefore require a higher degree of exporter awareness of, and compliance with, export licensing requirements than physical transfers of goods, software and technology. Exporters need to be encouraged to observe the record-keeping requirements of the Regulation. Such discipline will also help them to self-audit their transfers and should complement their efforts to protect proprietary information.

Compliance visits by national authorities

The purpose of compliance visits is to measure 'best practice' and compliance with export controls. Companies being visited will need to be able to demonstrate - an understanding of the Regulation and associated national export control legislation, as it relates to their activities. They will also need to demonstrate how they comply with these controls (for example any training or awareness activity arranged for engineers and other staff to explain what they need to do before making an electronic transfer).

[1] In compliance with Member States' legislation, and in accordance with their international obligations and in full respect of all fundamental rights, some EU Member States may consider the interception, by authorities mandated by law or on the basis of specific suspicions concerning illegal activities and under judicial control-, of telecommunications and mail surveillance are common investigative measures and – in general – valuable means of obtaining evidence in criminal proceedings.
Furthermore, the interception of telecommunications is effective in preventing the illegal export of goods. It may also serve to prevent illegal intangible transfers of technology and software.
Co-operation with intelligence services is important with a view to facilitating the exchange of information on potential violations.

During a compliance check it may be worthwhile approaching and questioning employees who have been made aware of the controls to check their knowledge is up to date.

Compliance visits will focus attention on ensuring that the parameters of authorisations have not been breached – i.e., that electronic transfers did not go beyond the type of technology that was licensed, or to bodies that were not specified on the end user undertaking. This will include ensuring that engineers or others who transfer technology are aware of the parameters of relevant authorisations-.

Auditing companies and institutions

To conduct audits of companies and institutions, audit officers require among other things:

- the necessary statutory powers of audit, and
- know-how on conducting audits with a view to ensuring compliance with regulations on intangible transfers.

Necessary powers of audit include the following:

- the right to demand information to verify compliance with export control regulations;
- the duty of the audited to supply this information;
- the right to inspect business documents and to use the computer network of the entity to search for information; and
- the right to enter business premises for this purpose.

If all transfers that require licences are documented, this facilitates audits. Industry, academic institutions and individuals should be obliged to keep certain registers or records of licensable electronic transfers of software and technology for an appropriate time period (minimum of 3 years). Record keeping requirements may vary for different types of licences. Records include in particular commercial documents such as invoices and dispatch notes that contain a description of the item and identify the exporter, the consignee, and, where known, the end-user.

Audits of companies and institutions to ensure compliance include the following:

- Audit officers should look for situations where an entity would typically transfer controlled technology or software by electronic means.

The following may indicate that the company is involved in electronic transfers of software or technology:

- the company sells software that is subject to export control;
- the company's homepage/intranet enables software to be downloaded when specific passwords are entered;
- the sale of the company's products typically requires the additional transfer of technology and/or software;
- the company sends engineers or technicians abroad to:
  - pick up equipment that is subject to export control,
  - provide or obtain training to use such equipment,
  - build installations, or
  - provide maintenance, upgrading or repair services;

- the company has applied for export licences for software and technology in the past, also bundled with licences for corresponding machines or equipment.

If an entity is involved in intangible transfers of software and technology, it would aim at ensuring that the company or institution:

- is familiar with export control legislation and precisely classify all the listed items they deal with;
- has a system in place to ensure that all staff are aware of the export control issue and adhere to the required procedure for making a transfer of technology and/or software;
- assigns clear responsibilities for export controls (preferably involving senior staff) and
- has in place a system to ensure that licences cover all relevant transfers of software and technology.

Audit officers may examine the following documents to measure compliance:

- contracts, software licence agreements, service or maintenance agreements;
- invoices, bank transfers, letters of credit etc. for transfers against payment;
- internal offset accounts for gratuitous transfers (warranty, fair dealing, transfers within a corporate group);
- travel reports, travel logs;
- acceptance negotiations;
- contacts with the information recipient prior to, and after, the respective transfer;
- server protocols (information on the possible transfer of technology abroad).

To be able to identify intangible transfers in server protocols and other electronic sources, audit officers will need to call on specialist advice and expertise.

Post transfer monitoring by national authorities

Post-transfer monitoring to detect unauthorised transfers is likely to be the main area of enforcement activity. In the absence of comprehensive records of transactions tell tale signs may be available to the investigator in business documents, internal communication papers and financial transactions. Those investigating breaches of the controls will also need to be able to call on specialist expertise to detect, seize and recover computer evidence although in many instances the most successful enforcement actions have stemmed from human intelligence when the authorities have been informed of an illegal activity.

Awareness

For the controls to work it is essential for national authorities to:

- Reach out to exporters, in particular those who are more likely to use intangible means to export controlled technologies to third countries and encourage "buy-in" by explaining clearly the necessity for them (risk of diversion/risk of loss of Intellectual Property Rights and revenues; application of EU legislation and the national penalties in place for non-compliance); their purpose and the crucial role that exporters play in the process. It is particularly important to identify SMEs dealing with new technologies that may be unaware of export control issues.

- Conduct regular post-export monitoring of industry compliance.

Awareness-raising and training efforts should focus on entities that are found to be significantly lacking in compliance. If it appears that export controls have been violated investigation authorities should be informed.