ECONOMIC COMMISSION FOR EUROPE

INLAND TRANSPORT COMMITTEE

Multidisciplinary Group of Experts on Inland Transport Security

Second session
Geneva, 9-10 October 2007
Item 4 of the provisional agenda

Informal document AC.11 No. 6 (2007)

20 September 2007

ENGLISH ONLY

REGULATORY INITIATIVES AT THE INTERNATIONAL LEVEL

Submitted by the European Commission

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
TAXATION AND CUSTOMS UNION
Customs Policy
Risk Management, Security and specific controls

Brussels, 29 June 2007

TAXUD/2006/1450

AUTHORISED ECONOMIC OPERATORS

GUIDELINES

Table of Content

Table of Content 3

PART 1, Section I 6

Introduction 6
I.1 How to use these guidelines? 7
I.2 AEO – Customs Simplifications: 7
I.3 AEO – Security and Safety: 8
I.4 AEO – Customs Simplifications / Security and Safety: 8
I.5 Who can become an AEO? 8

PART 1, Section II 9
How to audit 9
II.1 General 9
II.2 SME 9
II.3 Factors facilitating the authorisation process 10
II.3.1 Existing customs authorisations 11
II.3.2 Certifications and conclusions provided by experts 11
II.3.3 Parent/subsidiary companies with common system/procedures 12

PART 1, Section III 13

AEO Benefits 13
III.1 Fewer physical and document-based controls 13
III.2 Priory treatment of consignments if selected for control 13
III.3 Choice of the place of controls 14
III.4 Easier admittance to customs simplifications 14
III.5 Reduced data set for summary declarations 14
III.6 Prior notification 14
III.7 Indirect benefits 15
III.8 Improved relations with Customs 16
III.9 Recognised as a secure and safe business partner 16
III.10 Mutual recognition 16

PART 1, Section IV 17

The international supply chain and the concept of security 17
IV.1 Business Partners 17
IV.2 Security requirements for Business Partners 17
IV.3 Stakeholders in an international supply chain 19
IV.3.1 Manufacturer 20
IV.3.2 Exporter 20
IV.3.3 Freight Forwarder 20
IV.3.4 Warehouse keeper 20

IV.3.5 Customs Agent 21
IV.3.6 Carrier 21
IV.3.7 Importer 22
IV.4 Terms of delivery (INCOTERMS 2000) in relationship with supply chain security 23

PART 1, Section V 24

Determination of the competent Member State for submitting an AEO application 24
V.1 General 24
V.2 Multinational companies: subsidiaries 24
V.3 Multinational or big companies: branches 25
V.4 Accessibility of customs related documentation 25

PART 1, Section VI 27

Monitoring 27
VI.1 General 27
VI.2 Risk Management Audit Plans 27

PART 2, Section I 29

I.1 The criteria 29
I.2 The risks and the points for attention 30

I.2.1 Section I Company's information 30
I.2.1.1 Subsection 1 Volume of business 31
I.2.1.2 Subsection 2 Statistics on customs matters 32

I.2.2 Section II Compliance record 35
I.2.2.1 Subsection 1 Compliance history as regards customs authorities and other relevant governmental authorities 36
I.2.1.2 Subsection 2 Intelligence information 37

I.2.3 Section III The applicants accounting and logistical system 38
I.2.3.1 Subsection 1 Audit trail 39
I.2.3.2 Subsection 2 Accounting system 40
I.2.3.3 Subsection 3 Internal control system 43
I.2.3.4 Subsection 4 Flow of goods 45
I.2.3.5 Subsection 5 Customs routines 48
I.2.3.6 Subsection 6 Procedures as regards back-up, recovery and fall-back and archival options 49
I.2.3.7 Subsection 7 Information security – protection of computer systems 50
I.2.3.8 Subsection 8 Information security – documentation security 52

I.2.4 Section IV Financial solvency 54
I.2.4.1 Subsection 1 Insolvency 56

I.2.5 Section V Safety and security requirements 57
I.2.5.1 Subsection 1 Security assessment conducted by the economic operator (self assessment) 57
I.2.5.2 Subsection 2 Entry and access to premises 59
I.2.5.3 Subsection 3 Physical security 60
I.2.5.4 Subsection 4 Cargo units 62
I.2.5.5 Subsection5 Logistical processes 64
I.2.5.6 Subsection 6 Non-fiscal requirements 65
I.2.5.7 Subsection 7 Incoming goods 66
I.2.5.8 Subsection 8 Storage of goods 69
I.2.5.9 Subsection 9 Production of goods 70
I.2.5.10 Subsection 10 Loading of goods 71
I.2.5.11 Subsection 11 Security requirements business partners 74
I.2.5.12 Subsection 12 Personnel security 75
I.2.5.13 Subsection 13 External services 76

PART 3 77

I.1. Table of criteria that apply to the different actors in the supply chain 77
I.2. Abbreviations 84

PART 1, Section I

Introduction

As specified in the Commission's Communication on a simple and paperless environment for Customs and Trade[1], and as requested by the representatives of the Member States' customs authorities, guidelines should be drawn up for both customs authorities and economic operators to ensure common understanding and uniform application of the new customs legislation related to the AEO concept, and to guarantee transparency and an equal treatment of economic operators.[2]

These Guidelines do not constitute a legally binding act and are of an explanatory nature. Their purpose is to provide a tool to facilitate the correct application by Member States of the new legal provisions on Authorised Economic Operators. Please consult TAXUD customs and security website http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/index_en.htm to find the latest version of the AEO Guidelines.

The AEO Guidelines will need to be further developed and explained with best practises after the AEO provisions have become applicable. Without practical experience and in view of the very specific situation of and in particular the divergences among multinational companies and SME's, it is at this stage difficult to provide more guidance. Best practises can be introduced in the future when we have more practical experience of using the AEO Guidelines[3].

This document provides explanatory notes on the qualifying criteria for receiving the AEO status pursuant to Article 5a of the Community Customs Code as amended by Regulation (EC) no. 648/2005 (further on: CC) and Articles 14a-14q of its Implementing Provisions as amended by Regulation (EC) no. 1875/2006 (further on: CCIP).

There is no obligation for economic operators to become AEOs, it is a matter of the operators' own choice based on their specific situation. Nor is there any obligation for AEOs to require that their business partners have also to obtain AEO status.[4]

An Authorised Economic Operator can be defined as an economic operator who is reliable throughout the Community in the context of his customs related operations, and, therefore, is entitled to enjoy benefits throughout the Community. An AEO certificate, as laid down in Article 14b of the CCIP, provides either an easier admittance to customs simplifications, or it entitles the holder to facilitations concerning security and safety controls. In addition, there are benefits which are open to all categories of AEO, such as, amongst others, fewer physical and document based customs controls (unless other Community legislation prescribes a fixed amount).
Economic operators can also request a joint certificate ("customs simplifications" together with "security and safety") comprising all benefits referred to above.

---

[1] OJ C/2004/96 p. 10.

[2] In order to provide a Community-wide approach, the indicators and risk descriptions in these Guidelines were based on the COMPACT framework establishing a Community "best practice" method to assess risks for the implementation of customs regulations, including simplified procedures. Additionally a new section for safety and security standards has been added to Part 2 of these Guidelines.

[3] The Customs Code Committee on General Customs Rules will be the forum to discuss and amend the AEO Guidelines.

[4] Please see further clarifications in Part 1 Section IV.

I.1 How to use these guidelines?

Part 1 of the Guidelines contains explanations and examples which may assist in the AEO decision making process both for customs authorities and economic operators.

Part 2 of the Guidelines contains a questionnaire providing a list of points for attention to assist both customs authorities and economic operators to assess whether the AEO criteria are met or not. There is more then one way to address the issues specified in the questionnaire: the same requirements can be complied with using different means and methods.

In general, Part 2 of the Guidelines contains the following working method which can be used together with the AEO COMPACT model[5] describing a risk assessment methodology for AEO applicants:

> The aim is to assess the existing risks for the individual applicant, in accordance with the table at the end of the Guidelines. This means that the focus is only on the relevant risks and relevant points for attention; **applicants should not give an answer on each and every question if the information is already known to the customs authority or when the question is not relevant for the specific situation of the applicant.**
>
> All risk indicators in Part 2 of the Guidelines are linked to a risk description and to one or several points for attention.
>
> The risk descriptions give a clarification whether an indicator may be of importance.
>
> The points for attention can be used to detect if risks are actually relevant for a specific individual operator and to investigate what measures the operator has taken to deal with those risks.

I.2 AEO – Customs Simplifications:

An AEO Certificate - Customs Simplifications is issued to any economic operator established in the Community who fulfils the criteria of customs compliance, appropriate record-keeping standards and financial solvency. These criteria are further outlined in Sections II, III and IV of the Guidelines.

The holder of this certificate is entitled to:

- easier admittance to customs simplifications listed in Article 14b (1) of CCIP;
- fewer physical and document-based controls;
- priority treatment if selected for control;
- possibility to request a specific place for such control.

---

5 http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/index_en.htm#auth_eco

I.3 AEO – Security and Safety:

An AEO Certificate – Security and Safety is issued to any economic operator established in the Community[6] who fulfils the criteria of customs compliance, appropriate record-keeping standards, financial solvency, and maintains appropriate security and safety standards. The security and safety standards are described in Section V.

The holder of this certificate is entitled to:

- possibility of prior notification as described in Article 14b (2) of CCIP;
- reduced data set for summary declarations as specified in Article 14b (3) of CCIP;
- fewer physical and document-based controls;
- priority treatment if selected for control;
- possibility to request a specific place for such control

In the development of the AEO/Security and Safety requirements, the WCO SAFE Framework, existing security standards for maritime and air transport and ISO/PAS 28001 have been studied and where possible integrated. The integration of the WCO SAFE Framework was very important, as mutual recognition of secure AEO status could not be ensured without a globally recognised common base. Furthermore, in order to avoid unnecessary duplication of legal requirements on international and European recognised security and/or safety certificates in maritime, air cargo and surface freight transport, the relevant Commission services worked closely together. In this way requirements can be compatible enabling the authorities to recognise each others' security certifications.

I.4 AEO – Customs Simplifications / Security and Safety:

An AEO Certificate Customs Simplifications / Security and Safety is issued to any economic operator established in the Community who fulfils the criteria of customs compliance, appropriate record-keeping standards, financial solvency, and maintains appropriate security and safety standards and who wants to benefit from all AEO benefits.

The holder of this certificate is entitled to all benefits as listed in I.2 and I.3 above

I.5 Who can become an AEO?

Applications for AEO status may only be accepted from economic operators as defined in Article 1.12 of CCIP, according to which: “Economic operator means: a person who, in the course of his business, is involved in activities covered by customs legislation”.

On the basis of this definition an EU based supplier not involved in customs activities that supplies raw materials already in free circulation to an EU based manufacturer may not qualify to apply for AEO status. Similarly, in this case, a transport operator that moves only free circulation goods within the customs territory of the Community[7] may not qualify to apply for AEO status.

The definition of economic operator does not restrict the notion of "involvement in activities covered by customs legislation" to direct involvement only. A manufacturer producing goods to be exported can apply for an AEO status even if the export formalities are performed by another person.

The concept of AEO – Security and Safety is closely linked to supply chain management. Operators who are handling goods subject to customs supervision or handling data related to these goods can apply for AEO – Security and Safety certificate.

---

[6] Exception from the general rule of being established in the Community is provided for in Articles 14g and 14k (2) CCIP. The exception relates only to AEO Security and Safety.

[7] It is also supposed that he is not involved in the proof of Community status of the transported goods pursuant to Article 313 of CCIP

PART 1, Section II

How to audit

II.1 General

The number of hours required to carry out an AEO audit will vary according to a number of factors including:

- the size and complexity of the applicants operations;
- their preparation and records;
- existing information and authorisations held by the customs authorities (see II.3.2);
- any need for consultation between customs authorities;
- the need, where necessary, to consult with other governmental authorities.

In many cases the customs authorities will have direct access to a lot of information already held on the applicant, such as:

- information gathered when economic operators have applied for customs authorisations;
- information from customs audits; and
- information contained in the customs computerised systems about the daily use of customs procedures by the economic operator.

Customs authorities should use this information as much as possible in the AEO authorisation process in order to re-use information already at hand. This will ensure that the authorisation process can be conducted in an efficient manner.

If the applicant established in the Community is the holder of a simplified procedure authorisation, several parts of the AEO criteria have already been examined when the simplification authorisation was being granted. This fact should be taken into consideration when preparing an audit.

Customs authorities will also receive a lot of information about the applicant with his application. The Explanatory Notes for completion of the Application form in Annex 1C of CCIP contain the list of general information to be supplied by the applicant with his application.

Also, it is expected and recommended that applicants will make appropriate preparations in advance of the audit. It is essential that the economic operator ensures that there is a smooth and coordinated flow of communication between its relevant divisions, in order to allow for an efficient audit process.

II.2 SME

Small and medium sized enterprises are defined in Commission Recommendation of 6 May 2003 concerning the definition of micro-, small and medium-sized enterprises[8], according to which:

1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.

2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

[8] OJ L 124/2003

3. Within the SME category, a micro-enterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

Article 14a (2) of CCIP lays down the legal obligation that "the customs authorities shall take due account of the specific characteristics of economic operators, in particular of small and medium-sized companies."

The AEO criteria apply to all businesses regardless of their size. However, the means to achieve compliance will vary and be in direct relation to the size and complexity of the business, type of goods handled etc.

For example, all applicants seeking AEO/Security and Safety authorisation will have to demonstrate the adequacy of the physical security of their premises. This may include:

- a large manufacturer with a perimeter wall/fence, security guards, and CCTV (close circuit TV systems) cameras etc;
- a customs agent operating from a single room in a building with locks on doors, windows and filing cabinets;

As a further example, the requirement of identifying authorised persons (employees, visitors) could be carried out by an SME by other means than the use of badges.

Another example, related to the record-keeping requirement: all applicants seeking an AEO certificate - Customs Simplifications will have to demonstrate a good record-keeping system to facilitate audit-based customs controls. This may include:

- a large applicant having an integrated electronic record-keeping system directly facilitating for customs authorities to audit;
- an SME having only a simplified and paper-based system of record-keeping.

For further examples please see:
- Part 1 Section IV.2
- Part 2 Section III footnote 18
- Section IV Introduction.

II.3 Factors facilitating the authorisation process

In order to speed up the processing of applications, customs authorities should use, wherever possible, information they already hold on AEO applicants, in order to reduce the time needed for pre-audit. This will include information from:

- previous applications for customs authorisations;
- information which has already been communicated to the customs authority;
- customs audits;
- customs procedures used/declarations made by the applicant;
- self-assessment carried out by the applicant before submitting the application;
- existing standards held by the applicant; and
- existing conclusions of the relevant experts as laid down in Article 14n (2) of CCIP.

However, customs may need to re-check the criteria already fulfilled to ensure it is still valid.

In addition, customs authorities shall also take into account certain internationally recognised standards relevant to AEO authorisation which the applicant has attained and notified to them. (A specific column for possible related standards is added to the questionnaire, for providing guidance to customs authorities. The list of standards is not exhaustive.)

II.3.1 Existing customs authorisations

When an economic operator is applying for an AEO Certificate, the assessment of criteria already examined for other customs authorisations should be taken into account. This will reduce the time needed for the audit. However, the criteria already fulfilled may need to be checked to ascertain that they are still valid.

II.3.2 Certifications and conclusions provided by experts

The legislation ensures automatic recognition of safety and security standards for Regulated Agents [Article 14k (3) of CCIP]. This automatic recognition should apply to those premises of the applicant which acquired the Regulated Agent status.

As laid down in Article 14k (4) of CCIP, security and safety criteria shall also be deemed to be met to the extent that the criteria for issuing a certificate are identical or correspond to those laid down in the CCIP, if the applicant, established in the Community, is the holder of any of the following:

- an internationally recognised security and/or safety certificate issued on the basis of international conventions;
- an European security and/or safety certificate issued on the basis of Community legislation;
- an International Standard of the International Organisation for Standardisation;
- an European Standard of the European Standards Organisations.

This shall only be valid for certifications issued by internationally accredited certifiers[9] or national competent authorities. Certifications issued by others may be taken into account in accordance with Article 14n (2) of CCIP where appropriate.

The Guidelines have been updated therefore with a column for existing international standards. (However, in the absence of practical experiences, the list is not exhaustive.) This would mean that the audit will take less time and it will be easier for the already compliant economic operator to assess, before submitting an application, that he meets those criteria which are identical or comparable, to the extent of the similarities between the international certificates' and the AEO criteria.

The most relevant standards which have been identified until now are various ISO standards (for example ISO 9001, 14001, 20858, 28000, 28001, 28004), and the ISPS Code[10]. Having a given ISO-certification does not automatically mean, that the specific AEO criteria are met. Sometimes a given ISO-certification does comply with the AEO criteria; other times it does not fully comply and additional requirements must be fulfilled by the applicant.

Verifiable compliance with security requirements and standards set by intergovernmental organisations, such as IMO, UNECE and ICAO, may also constitute partial or complete compliance with the security criteria, to the extent the requirements are identical or comparable.

Also, customs authorities may, as laid down in Article 14n (2) of CCIP, accept conclusions provided by an expert in the fields of record-keeping, financial solvency or security and safety standards.

---

[9] MLA (Multilateral Recognition Arrangement) or MRA (Mutual Recognition Arrangement). See also www.european-accreditation.org

[10] These standards can be regarded as security and safety certificates according to Art. 14 k (4) and Article 14k (2) last paragraph; and as conclusions by an expert according to Art. 14 n (2) if they are related to record-keeping.

II.3.3 Parent/subsidiary companies with common system/procedures

Each subsidiary wishing to apply for AEO status shall complete a separate application form.[11]

However, if the subsidiary companies are applying the same corporate standards/procedures for their customs related activities, the **questionnaire**[12], contained in Part Two of the Guidelines could be completed by the parent company on behalf of all the subsidiaries that have submitted an application.

In this case the customs authority may receive many application forms but only one completed questionnaire covering all applications in relation to criteria which can be common for all subsidiaries, mainly those contained in Part 2. Sections 3 and 5.

This solution is applicable not only to situations where the parent company and its subsidiary companies are established in the same Member State. It is also applicable to situations where a parent company has subsidiaries in other Member States. National customs authorities should arrange their AEO application processes, including consultation procedures, where necessary, with other customs administrations, accordingly.

This is especially recommended in situations where the parent company and its subsidiaries are already holders of Single European Authorisation.

[11] See also explanation in Part One Section V.1. Definition of subsidiaries can be found in Council Directive 90/435/EEC as well as in the national legislation.

[12] The use of the questionnaire is explained in Section I.1.

PART 1, Section III

AEO Benefits

It should be noted here that an AEO Certificate is issued to the applicant and not to his clients. Therefore, benefits can be used by the AEO only. This is a general principle for all types of operators in the international supply chain.

The AEO benefits, dependant on the type of the certificate, are summarized below.[13]

III.1 Fewer physical and document-based controls

This benefit will apply from 1 January 2008 and is applicable to all categories of AEO.

Article 14b (4) of CCIP lays down that an AEO shall be subject to fewer physical and document-based controls than other economic operators. This means that an AEO shall have a lower risk score and enjoy faster border crossings (relevant to the type of certificate).

The holder of an AEO certificate shall have a lower risk score in all Member States as the status is recognised in all MS pursuant to Article 5a of the Community Customs Code. The lower risk score should be incorporated into the risk management and customs movements systems in order to allow for this benefit as regards the AEO's daily operations.

III.2 Priority treatment of consignments if selected for control

This benefit will apply from 1 January 2008 and is applicable to all categories of AEO.

When, following risk analysis, the customs office selects for a further examination a consignment covered by a summary or a customs declaration lodged by an AEO, it shall carry out the necessary controls as a matter of priority. This means that the consignment should be the first to be controlled if others are also selected from non-AEO's.

[13] See also Article 14b of CCIP as amended by Regulation 1875/2006.

III.3 Choice of the place of controls

This benefit will apply from 1 January 2008 and is applicable to all categories of AEO.

Customs control can be asked by an AEO to be diverted to another place where it can lead to the shortest delay or less costs for the AEO. However, this is subject to an agreement with the customs authority concerned.

III.4 Easier admittance to customs simplifications

This benefit will apply from 1 January 2008 and is applicable to holders of AEO Certificate - Customs Simplifications or of AEO Certificate – Customs Simplifications/Security and Safety.

Economic operators do not need to have AEO status in order to get an authorisation for a simplification provided for under the customs rules. However, if the person requesting a simplification is the holder of an AEO certificate – Customs Simplifications (or of a joint certificate), the customs authority shall not re-examine those conditions which have already been examined when granting the AEO status.

The criteria which are deemed to be met by an AEO can be found at the appropriate Article of the specific simplification, a list of which is provided here:

Local clearance	Article 264 (3)
Simplified declaration	Articles 261 (4); 270 (5)
Regular shipping service	Article 313b (3a)
Proof of Community status/authorised consignor	Article 373 (3)
Proof of Community status/Art. 324e	Article 373 (3)
Transit simplifications	Articles 373 (3) and 454a (5)
T5 control copy/Art. 912g	Not specified but inherent in Article 912g (4)

III.5 Reduced data set for summary declarations

This benefit will apply from 1 July 2009 and is applicable to holders of AEO Certificate – Security and Safety or of AEO Certificate – Customs Simplifications/Security and Safety.

AEO-importers and AEO-exporters are automatically entitled to submit summary declarations with a reduced set of data elements. The reduced data-set is shown in Table 5 of Annex 30A of CCIP.

AEO-carriers, AEO-freight forwarders and AEO-customs agents may use this benefit only for their clients who are holders of AEO Certificate – Security and Safety or of AEO Certificate – Customs Simplifications/Security and Safety.

III.6 Prior notification

This benefit will apply from 1 July 2009 and is applicable to holders of AEO Certificate – Security and Safety or of a joint certificate.

When a summary declaration has been lodged by an AEO, the competent customs office may, before the arrival/departure of the goods into/from the Community, notify the AEO when, as a result of security and safety risk analysis, the consignment has been selected for further physical control.

This notice shall only be provided where it does not jeopardise the control to be carried out.
The customs authorities may, however, carry out a physical control even where an AEO has not been notified.

III.7 Indirect benefits

Any economic operator that meets the criteria and becomes an AEO may derive benefits that are not directly linked to the customs side of his business.

Investment by operators in increasing their security and safety standards may yield positive effects in the following areas: Visibility and Tracking, Personnel Security, Standards Development, Supplier Selection and Investment, Transportation and Conveyance Security, Building Organizational Infrastructure Awareness and Capabilities, Collaboration Among Supply Chain Parties, Proactive Technology Investments and Voluntary Security Compliance.

Some examples of the indirect benefits that may result from these positive effects could be as follows:

- reduced theft and losses;
- fewer delayed shipments;
- improved planning;
- improved customer loyalty;
- improved employee commitment;
- reduced security and safety incidents;
- lower inspection costs of suppliers and increased co-operation;
- reduced crime and vandalism;
- reduced problems through recognition of employees;
- improved security and communication between supply chain partners.

III.8 Improved relations with Customs

In order to introduce good co-operation between customs authorities and the AEO, it is recommended that the AEO has access to a service centre or a contact person in the customs authority to which it can address its questions. The service centre might not be able to provide all answers on all questions but would act as an initial point of contact to the customs authorities and guide the AEO on how best to proceed and whom to contact.

III.9 Recognised as a secure and safe business partner

An AEO who meets the security and safety criteria is considered to be a secure and safe partner in the supply chain. This means that the AEO does everything in his power to reduce threats in the supply chain where he is involved. The AEO status enhances his reputation.
Furthermore, being a secure and safe partner in the supply chain allows facilitations from security controls.

The AEO could therefore be chosen as a business partner, instead of a non-AEO, when another economic operator is looking for new business partners.

III.10 Mutual recognition

The Community's objective is to reach mutual recognition of the AEO Security and Safety with all countries who implement an AEO program or equivalent. Thus, an AEO Security and Safety /EC would get the same benefits in third countries as those AEO's that are established in those countries. Globally, this would ensure more predictability for his international trade operations.

Subject to the provisions of the relevant international agreement between the EC and third country, an AEO Security and Safety/EC might not need to apply for the relevant AEO/third country status in that third country, because the EC certificate might be recognised by that third party.

Mutual recognition, not only related to AEO's but also to control standards and controls is essential. The fact that a high number of WCO members have committed to implement the WCO SAFE framework, the implementation of comparable measures on an international scale and thus mutual recognition will be achieved in certain areas of the world.

PART 1, Section IV

The international supply chain and the concept of security

This chapter concerns applicants for AEO Certificate – Security and Safety or for a joint certificate.

The international end-to-end supply chain from a customs perspective represents the process from manufacturing goods destined for export until delivery of the goods to the party to whom the goods are actually consigned in another customs territory (being the customs territory of the EC or another customs territory). The international supply chain is not a discrete identifiable entity. It is a series of ad hoc constructs comprised of operators representing various trade industry segments. In some cases the operators are all known and a long time relationship may exist, whilst in other cases operators may change frequently or may only be assembled for a single shipment.

IV.1 Business Partners

From a customs perspective business partners as mentioned in article 14k(1)(e) of CCIP may have the option to apply for AEO status[14] but if they choose not to exercise that option they should provide assurances to the other members of the supply chain regarding safety and security. All operators in the supply chain that fall between the exporter/manufacturer and the consignee may be regarded as business partners.

IV.2 Security requirements for Business Partners

Article 14k (1) (e) of CCIP stipulates that security and safety standards in relation to business partners shall be considered to be appropriate if "the applicant has implemented measures allowing a clear identification of his business partners in order to secure international supply chain."

Authorised Economic Operators can only be held responsible for their part of the supply chain, for the goods which are under their custody and for the facilities they operate. However, they are also dependent on the security standards of their business partners in order to ensure the security of the goods in their custody.

[14] If they are established in the Community, as a general principle

In order to meet the requirement AEOs should, when entering into new contractual arrangements with a business partner encourage the other contracting party to assess and enhance their supply chain security and, to the extent practical for their business model, include such language in those contractual arrangements.

In addition, the AEO is recommended to retain documentation in support of this aspect to demonstrate their efforts to ensure that their business partners are meeting these requirements. The AEO could also review relevant commercial information relating to the other contracting party before entering into contractual relations.

Examples of how an AEO could enhance his supply chain security are:

- the supply chain can be considered as fully secure if the AEO is responsible for the whole supply chain e.g. the AEO acts as the exporter and carrier;
- the AEO works together with other AEO's or equivalent[15];
- the AEO enters into contractual arrangements on security with his business partners;
- subcontractors (for example transporters) used by the AEO are chosen on the basis of their adherence to certain security rules;
- containers are sealed with "high security seals" of norm ISO-PAS 17712;
- the containers are inspected at the subcontractor's premises, the terminal and recipient premises to verify that they have been sealed correctly;
- general information from bodies responsible for the registration of companies (where possible) and the partner's products (risky and sensitive goods etc.) are considered before entering into contractual arrangements;
- the AEO asks for a security declaration[16];
- use facilities that are regulated by international or European security certificates (for example ISPS Code and Regulated Agents).

Whenever an AEO has information that one of his business partners who is part of the international supply chain does not have established appropriate security and safety standards, he will immediately take appropriate measures, to the extent possible, to enhance supply chain security.

Regarding consignments taken over from unknown business partners: it is recommended that the AEO takes measures to guarantee that security risks related to unknown business partners can be limited to an acceptable level. In case the AEO discovers compliance difficulties, it shall contact the customs authorities of such occurrences.

---

[15] The summary declaration submitted by the AEO will always reflect this situation, as the relevant AEO identification numbers will be indicated at each box for each AEO business partner (for example, the boxes for "carrier", "consignee", "consignor").

[16] As a way of example, please see ISO/PAS 28001, Part 3.18: "a security declaration is a documented commitment by a business partner, which specifies security measures implemented by that business partner, including, at a minimum, how goods and physical instruments of international trade are safeguarded, associated information is protected and security measures are demonstrated and verified".

IV.3 Stakeholders in an international supply chain

In the international supply chain there are different stakeholders which have, according to their part in this chain, different responsibilities. To assess the operator's supply chain security capabilities, different sets of criteria have to be fulfilled depending on the operator's responsibility within the supply chain. The different kind of economic operators and their different responsibilities in the international supply chain, relevant from a customs perspective, are therefore described below. The table of criteria comprising all sub-sections for stakeholders can be found in Part 3 of the Guidelines[17].

However, it is not possible at this stage to list all actors in the international supply chain. The list below can be up-dated once customs authorities acquired more practical experience on the application of the AEO system.

[17] Please see further detailed explanation in Part 3.

IV.3.1 Manufacturer

A manufacturer's responsibility in the international supply chain can be regarded as follows:

- Ensure a safe and secure manufacturing process for its products.
- Ensure a safe and secure supply of its products to its clients.

IV.3.2 Exporter

An exporter, pursuant to Article 788 of CCIP, is the person on whose behalf the export declaration is made and who is the owner of the goods or has a similar right of disposal over them at the time when the declaration is accepted. Where the ownership or a similar right of disposal over the goods belongs to a person established outside the Community pursuant to the contract on which the export is based, the exporter shall be considered to be the contracting party established in the Community.

An exporter's responsibility in the international supply chain can be regarded as follows:

- Responsible for the correctness of the export declaration and for its timely lodgement, if the export declaration is lodged by the exporter.
- Responsible, if the export declaration is lodged by the exporter, for lodging an export declaration which contains the data elements of the exit summary declaration, once the provisions on exit summary declaration will become applicable from 1 July 2009.
- Apply the legal export formalities in accordance with the customs rules, including commercial policy measures and where appropriate, export duties.
- Ensure a secure and safe supply of the goods to the carrier or freight forwarder or customs agent.

IV.3.3 Freight Forwarder

A freight forwarder organises the transportation of goods in international trade on behalf of an exporter, an importer or another person. In some cases, the freight forwarding applicant provides the service himself and acts as a carrier. A freight forwarder's typical activity can include: obtaining, checking and preparing documentation to meet customs requirements.

A freight forwarder's responsibility in the international supply chain can be regarded as follows:

- Apply the rules on transport formalities
- Ensure, if relevant, a secure and safe transport of goods
- Apply, if relevant, the rules on summary declarations in accordance with the legislation

IV.3.4 Warehouse keeper

A warehouse-keeper is a person authorised to operate a customs warehouse pursuant to Article 99 of the Community Customs Code, or a person operating a temporary storage facility pursuant to Article 51 (1) of the Code and Article 185 (1) of CCIP.

A warehouse-keeper's responsibility in the international supply chain can be regarded as follows:

- Ensure that while the goods are in a customs warehouse or in temporary storage, they are not removed from customs supervision.
- Fulfil the obligations that arise from the storage of goods covered by the customs warehousing procedure or by the rules on temporary storage.
- Comply with the particular conditions specified in the authorization for the customs warehouse or for the temporary storage facility.
- Provide adequate protection of the storage area against external intrusion.
- Provide adequate protection against unauthorized access to, substitution of and tampering with the goods.

IV.3.5 Customs Agent

A customs agent referred to in these AEO Guidelines means a customs representative as laid down in Article 5 of CC. A customs representative is acting on behalf of a person who is involved in customs related business activities (e.g. an importer or an exporter). A customs representative may act either in the name of this person (direct representation) or in his own name (indirect representation).[18]

A customs agent's responsibility in the international supply chain can be regarded as follows:

- Apply the necessary provisions in accordance with the customs rules specific for the type of representation, for placing the goods under a customs procedure.
- In case of indirect representation, responsible for the correctness of the customs or summary declaration and for its timely lodgement.

IV.3.6 Carrier

A carrier is the person actually transporting the goods or in charge of or responsible for the operation of the means of transport.

A carrier's responsibility in the international supply chain can be regarded as follows:

- Ensure a secure and safe transport of goods, in particular avoiding unauthorized access to and tampering with the means of transport and the goods being transported.
- Provide necessary transport documentation.
- Apply the necessary legal formalities in accordance with customs law.

[18] It should be noted, concerning the AEO Certificate – Security and Safety, that the security criteria are mainly focusing on securing the premises where the goods are stored or securing the containers. Only a limited number of criteria (such as "personnel security") can be met by those customs agents who are only dealing with producing customs declarations without warehousing or freight forwarding activities. Furthermore, there is no correlation between the type of representation (direct or indirect) and the range of work performed by a customs agent (customs documentation work only, or also warehousing, transporting etc).

IV.3.7 Importer

An importer is an operator on whose behalf an import declaration is made.

An importer's responsibility in the international supply chain can be regarded as follows:

- Responsible, if he has not appointed an indirect representative in his dealings with the customs authorities, for assigning the goods presented to customs a customs-approved treatment or use.
- Responsible, if the import declaration is lodged by the importer, for the correctness of the declaration and that it will be lodged in time.
- The importer can be the operator who is lodging the entry summary declaration when the relevant provisions will become applicable from 1 July 2009 and therefore could be responsible for the correct application of the rules on summary declarations.
- Apply the necessary legal formalities in accordance with customs rules relevant to the import of goods.
- Ensure a secure and safe receipt of goods, in particular avoiding unauthorized access to and tampering with the goods.

IV.4 Terms of delivery (INCOTERMS 2000) in relationship with supply chain security

It follows from the above, that an "importer", "exporter" or another party in the supply chain are defined in the customs law and the definitions have only a very limited link to terms of delivery.
Terms of delivery appear in the moment when a seller and a buyer enter into a contract. It is a tool one can use to increase the security in the business. Other parts of the contract may be additional safety requirements, such as pre-announcements of goods or the sealing procedure etc.
INCOTERMS ICC/ECE as well as their meaning is incorporated in Annex 38 of the CCIP (Title II, Box 20).

INCOTERMS provide a good guide as to what extent an operator can influence security in the supply chain. Therefore, in order to secure one's supply chain it is recommended that an AEO-buyer, taking its size and business environment into consideration, should only enter contracts that, give as much influence as possible regarding the choice of transportation providers (forwarders, carriers). This is because by having influence on the choice of transportation suppliers, the AEO-buyer knows which suppliers are committed to safeguard their supply chain and which are not. An AEO-exporter is recommended to do this the other way around.

However, customs authorities have to take the operations of SME's into consideration. This is a legal obligation pursuant to Article 14a (2) CCIP, which lays down that "the customs authorities shall take due account of the specific characteristics of economic operators, in particular of small and medium-sized companies."

SME don't have the same scope as larger companies to influence security in the supply chain. Customs authorities can't expect that an SME will have equal responsibility in the chain as a multinational operator. Remaining risks for an operator due to the different supply chains will be considered when customs authorities select consignments for security and safety controls.

Each case has to be assessed individually: even if an operator enters into a contract where he takes responsibility for the whole supply chain, a mapping of other potential risks (such as the sealing procedure) still remains.

PART 1, Section V

Determination of the competent Member State for submitting an AEO application

V.1 General

The Member State to which the AEO application should be submitted is determined in Article 14d of CCIP. The main idea is that the application should be submitted to the Member State which has the best knowledge of the applicant's customs related activities, which implies that an application is to be submitted to the Member State where:

- the applicant's main accounts related to the customs arrangements involved are held or accessible, and
- the customs related operations are conducted,

both conditions being to be fulfilled at the same time.

If it is not possible to determine the Member State on this basis, the application should be submitted to the Member State where the main accounts related to the customs arrangements involved are held or accessible.

In view of the modern trends in companies' organisational structures and business flows, as well as of the ongoing trend on outsourcing certain activities including accountancy, the correct decision is not always "at hand". The following guiding principles are recommended, before taking the final decision.

V.2 Multinational companies: subsidiaries

Multinational companies usually consist of a parent company and subsidiary companies, each of them being an individual legal person, i.e. an individual legal entity registered in the local company register according to the Member State's company law where the relevant subsidiary is established. Therefore, if a parent company would like to get the AEO status for a part or all of its subsidiaries, AEO applications must be submitted by all the subsidiary companies wishing to get the AEO status.

Example:
A parent company "P" is established in Germany. It has the following subsidiaries: subsidiary "S1" registered in Belgium, and a subsidiary "S2" registered in Austria. The parent company "P" is not carrying out any business related to customs rules, but his subsidiaries are involved in activities covered by customs legislation. Parent company "P" would like to get the AEO status for all the customs related activities carried out by his subsidiaries. The main accounts related to the customs arrangements involved as well as the customs related activities are performed in the Member States where the subsidiaries are registered.

The application has to be submitted by all the subsidiaries, in their own names:
Subsidiary "S1" has to submit an application in Belgium, and subsidiary "S2" an application in Austria.

V.3 Multinational or big companies: branches

According to company law, a "branch" is not an individual legal entity; it is an office/premise/another location of the company itself and forms part of the company's total assets. Such a company wishing to acquire the AEO status does not need to submit applications for all of its branches; it is sufficient to submit only one application in the Member State as described at the introductory part of this section.

Example no.1:
Company "C" has its headquarters in Belgium and holds its main accounts in Belgium too. The company is maintaining a warehouse "W" in France for its import-related operations. The main accounts related to the customs arrangements involved are kept by this warehouse.

The application has to be submitted by applicant "C" in France. In box 13 of the application form "France" should be indicated, and boxes 16 and 17 should contain the address of warehouse "W", whereas box 18 should relate to an address in Belgium.

Example no.2:
Company "A" is registered in France according to French company law. It constitutes the headquarters for the Europe-Middle East- Africa (EMEA) region and is situated in Paris, France. It is the shared services centre for the distributors, sales-offices, retail-chains and stores all across Europe, Middle East and Africa (EMEA) and houses the management and finance department. However no customs related activities are carried out on this site.

Company "A" has a branch in Belgium, which is the distribution centre for the whole EMEA region. All customs related activities and bookkeeping are done in Belgium. All relevant accounts related to customs arrangements are kept there.
Company "A" has several customs authorisations that are granted in Belgium, to be used in the branch activities:

- Warehouse type D
- Warehouse type C
- Authorized Consignor-Consignee
- Authorized Exporter
- Issuance of T2L declarations

To submit the AEO application in the correct Member State, first consider the place where the main accounts, related to the customs arrangements involved, are held.
This means: look at the main accounts, related to the customs arrangements involved, and not just the financial main accounts. The main accounts here include records and documentation enabling the customs authority to verify and monitor the conditions and the criteria necessary for obtaining the AEO certificate [Art 14d (1) last paragraph of CCIP].

Thus, in this case, even if company "A" is registered in France, according to Article 14d of CCIP the application should be submitted in Belgium.

V.4 Accessibility of customs related documentation

Paragraphs (1)(b) and (2)(b) of Article 14d CCIP are addressing the situation where a company is outsourcing its customs related accountancy to an entity in another Member State or in a third country. This practise is usual and legally allowed in many Member States. In these cases, the company is ensuring that the customs authority of the Member State where he is established has electronic access to the documentation held in another Member State or in a third country.

In these situations, the application has to be submitted in the Member State to which the company ensures the accessibility and where his logistical management activities are conducted, as well as (at least part of) his customs related activities are carried out. [Article 14d (1) (b) CCIP]

If the company carries out his customs related activities in another Member State, the application has to be submitted nevertheless in the Member State where accessibility of his main accounts related to the customs arrangements involved is ensured and his logistical management activities are conducted.[Article 14d (2)(b) CCIP]

Example no.1:

Company "C" is established in Sweden. It carries out all his business activities in Sweden, except that the accountancy is outsourced into Estonia. It ensures electronic access to his documentation to the Swedish customs authority as defined by the relevant rules in Sweden.

The AEO application is to be submitted in Sweden.

Example no. 2:

Company "C" is established in the UK. It out-sources its accountancy to Ireland and ensures electronic access to his documentation to the UK customs authority as defined by the relevant rules in the UK. It imports goods from Asia through Italy, but the general logistical management activities are still maintained in the UK.

The AEO application is to be submitted in the UK.

PART 1, Section VI

Monitoring

VI.1 General

Article 14q (4) of CCIP states that "The customs authorities shall monitor the compliance with the conditions and criteria to be met by the authorised economic operator".

This provision requires issuing customs authorities to ensure that they develop in conjunction with the AEO a system for monitoring the compliance with the conditions and criteria of the authorisation. Any control measures undertaken by the customs authorities should be recorded.

Customs authorities could comply with this provision in the following ways:

- The customs authority draws up an audit plan describing the way in which it intends to respond to the risks identified during the evaluation. Therefore, the audit plan will differ from operator to operator. The audit plan could include details of the following measures to be undertaken:
  - Random checking of declarations;
  - Any physical inspections of goods and/or audits to be undertaken;
  - Evaluation of any changes in company behaviour or trade patterns that come to notice.

- Request the operator to sign a set of conditions in advance of granting the AEO certificate, covering the operator's responsibilities in complying with the AEO conditions and criteria. The AEO is legally obliged to inform the competent customs offices of significant events that could affect his authorisation, including cases when there is a change in the condition of access to information or in the way the information is made available.

VI.2 Risk Management Audit Plans

The customs authority should draw up a follow-up and audit plan. The audit plan describes the way in which the customs authority intends to respond to the risks identified. All intended control measures, checking of declarations, physical inspections of goods and/or audits that will be carried out by the customs, should be described and planned in the audit plan.

The results of the control activities must be documented.

It is of great importance that the criteria and conditions of the AEO status are evaluated on a regular basis.

A number of elements, described below, play a role in this evaluation:

- **Results of controls**

The results of the control activities as described in the audit plan. These results can give an indication that risks are no longer sufficiently covered by the operator. The customs authorities should evaluate the results of the control activities on a regular basis. This may result in adjustments of the control approach.

- **Early warning signals**

Signals from the operator about changes in its activities, organisation or procedures. When granting the AEO status it should be agreed that the operator is obliged to report changes to the customs authorities.

- **Monitoring of risks**

  It is necessary that customs authorities check thoroughly that the operator is still in control of the risks. Are there any new risks? Is the quality of the administrative organisation and the internal control system still as good as it was during the time of the pre-audit? For this reason customs authorities must from time to time perform an evaluation audit.

If one of the elements of the evaluation leads to the conclusion that the operator is not or no longer in control of one or more risks, the customs authority informs the operator about that conclusion. The operator then must undertake improvement actions. It is again incumbent on the customs to assess these improvement actions. This can also lead to the conclusion that the AEO status should be suspended or revoked.

However, monitoring will also lead to a better understanding of the AEO's business which could even lead the customs authorities to recommend to the AEO a better, more efficient way of using the customs procedures or the customs rules in general.

PART 2, Section I

I.1 The criteria

Article 5a of CC[19] provides for the granting of the status of AEO to reliable traders that fulfil the criteria laid down in Article 5a (2) CC. The status of AEO shall be recognised by the customs authorities in all Member States.

AEO criteria:

— *an appropriate record of compliance with customs requirements*

— *a satisfactory system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls*

— *proven financial solvency and*

— *where applicable, appropriate security and safety standards."*

These criteria are further defined in the respective Articles 14h-14k of CCIP.

The following questionnaire provides a list of points for attention to assist both customs authorities and economic operators to assess whether the AEO criteria are met or not.

The questionnaire is divided into Sections. The first Section helps customs authorities to establish an overall image of the applicant from a "customs" perspective. Each further Section corresponds to a specific criterion described in Article 5a of CC and in the relevant Article of CCIP (for example, Section II. corresponds to Article 14h of CCIP – customs compliance). Most of the Sections are further divided into sub-sections which correspond to the specific sub-items of the relevant Article in the CCIP.

Applicants should not give an answer to each and every question if the information is already known to the customs authority or when the question is not relevant for the specific situation of the applicant. The questionnaire should also be read in conjunction with Part 3 that indicates which areas of the criteria apply to the different parties in the supply chain.

There is more then one way to address the issues specified in the questionnaire: the same requirements can be complied with using different means and methods.

In the case of newly established companies, the company might not have the ability to submit all information concerning questions related to his history. If the new company has been created in the form of a merger of already existing companies, general information about these companies as well as about their compliance would help the customs authorities to assess the risks related to the shortage of information.

[19] OJ L 117, 4.5.2005, p. 13

I.2 The risks and the points for attention

I.2.1 Section I Company's information

This section is a listing of information necessary for the customs authority to provide itself a "picture" of the applicant and its activities. Some of this information may already be available if the applicant has already received customs authorizations.

In order to proceed with the process of granting the AEO status the applicant has to submit details as laid down at the end of the Explanatory notes in Annex 1C of CCIP. The applicant could use the areas in this Section to ensure that the details are communicated and to facilitate the process of granting of the AEO status.

I.2.1.1 Subsection 1 Volume of business

1.01.	Indicator		Points for attention	
1.	Annual turnover (general)		What's the amount of the annual turnover (general) of the last 3 year(s)?	
2.	Profits and losses		What's the amount of the profits and losses of the applicant of the last 3 year(s)?	
3.	Stock capacity		What is the capacity (in square or cubic meters) of the storage facility?-	
4.	Purchases (foreign trade).		Provide an estimate (per supplier if relevant) of the volume (in terms of quantity and money) of the purchases expected in the next 2 years. State in this overview the description of the items.	
5.	Goods received in customs or fiscal warehouse		Provide an estimate (per customer if relevant) of the volume (in terms of quantity and money) of the goods received in customs or fiscal warehouse expected in the next 2 years. State in this overview the description of the items.	
6.	Goods used in the production process		Provide an estimate of the volume (in terms of quantity and money) of the goods used in the production process expected in the next 2 years. State in this the description of raw materials and semi-manufactured articles.	
7.	Outcome of the production process		Provide an estimate of the outcome of the production process (in terms of quantity and money) expected in the next 2 years. State in this overview the description of the items.	
8.	Sales (foreign trade)		Provide an estimate (per buyer if relevant) of the volume (in terms of quantity and money) of the sales expected in the next 2 years. State in this overview, the description of the items.	
9.	Goods removed from customs or fiscal warehouse		Provide an estimate (per customer if relevant) of the volume (in terms of quantity and money) of the goods removed from the customs warehouse expected in the next 2 years State in this overview the description of the items.	

I.2.1.2 Subsection 2 Statistics on customs matters

1.02.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Tariff classification	Incorrect classification of the goods. Incorrect duty rate.	In what way and by who are the goods classified (Tariff of goods, excise category, other levies)? Is there a separate file in which each article number is linked with a commodity code? If so, how and by whom is this file maintained. Does this file also contain the current rate? If so, who maintains this? What are the routines for classification of goods/new products? Provide an overview of all relevant article numbers in relation with the commodity code and rates (VAT, excise, import duty, CAP-goods). Provide a list of the operator's support (such as library of handbook) for classification.	
2.	% of import duties	Use of low duty tariff codes.	Provide an overview of the relevant rates linked with the goods codes.	
3.	% of VAT	Use of a low VAT tariff.	Provide an overview of the relevant rates linked with the goods codes.	
4.	% of excise	Use of low excise tariff codes.	Provide an overview of the relevant rates linked with the goods.	
5.	CAP (duties and refunds)	Use of low duty/high refund tariff codes.	Provide an overview of the relevant rates linked with the goods codes.	
6.	Preferential measures	Use of incorrect origin or incorrect tariff code.	Do preferential measures exist regarding to the goods the applicant deals with.	
7.	Antidumping duties	Use of incorrect tariff code or incorrect supplier.	Provide an overview of the relevant anti-dumping duties linked with the goods codes and manufacturer.	
8.	Origin / provenance of goods	Abuse of preferential tariffs. Avoid restrictions by use of wrong origin indication.	Provide an overview of the origin of the goods declared for import. Provide an overview of goods/article (numbers) in which the company appeals to preferential tariffs.	

1.02.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
			What are the routines for checking the correctness of country or origin of import goods? What are the routines for issuing proof of origin at export?	
9.	Customs/VAT value *Note: VAT only import and export related*	Incorrect customs value.	What are the routines to determine the customs and VAT value? What are the routines for declaring freight and insurance costs? In case of an agreement about the custom value (ruling) quote the reference and attach a copy of the ruling letter. The following aspects related to the customs value can be verified: ✓ The Inco terms used. ✓ Buyer and seller relationship in terms of the EC regulation and the influence the relationship may have on the price of the imported goods. ✓ Restrictions to the disposal of the goods by the buyer. ✓ If the sale or price is subject to some condition or consideration for which a value cannot be determined with respect to the goods being valued. ✓ Royalties and license fees related to the imported goods payable either directly or indirectly by the buyer as a condition of sale. ✓ Arrangements under which part of the proceeds of any subsequent resale, disposal or use accrues directly or indirectly to the seller. ✓ Costs incurred by the buyer (but not included in the price) in respect of commissions or brokerage (except buying commissions) or of containers and packaging. ✓ Goods and/or services supplied by the buyer free of	

1.02.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
			charge or at reduced cost for use in connection with the production and sale for export of the imported goods. ✓ Other costs than those associated with the delivery of the imported goods included in the price payable. ✓ In what way is the person who makes the declaration aware of possible costs not directly linked to a consignment?	

I.2.2 Section II Compliance record

Criterion**:**

An appropriate record of compliance with customs requirements
Article 14h of CCIP

The applying economic operator, the persons in charge of the applicant or exercising control over its management, and, if applicable, the applicant's legal representative in customs matters and the person responsible in the applicant company for customs matters should not have committed a serious infringement or repeated infringements of customs rules over the last 3 years preceding the submission of the application. However, the record of compliance may be considered as appropriate if the infringements can be considered to be of negligible importance in relation to the number or size of the customs related operations and do not create doubts concerning the good faith of the applicant.

The applicant's compliance could be judged on the basis of the records of the customs authority. If the persons exercising control over the management of the applicant company are established or resident in a third country, their compliance shall be judged on the basis of records and information that are available.

If the applicant has been established for less then 3 years, his compliance shall be judged on the basis of records and information that are available.

Minor Infringements

In order to establish what may be regarded as a minor infringement, the first guideline to be observed is that each case is different, and should be treated on its own merits against the background and size of the operator concerned. A minor infringement in one Member State may be a serious infringement in another Member State. It should be established whether the infringements are indicative of an underlying problem of a lack of knowledge of customs rules and procedures by the trader or are the consequence of negligence. If a decision is taken that the infringement may be regarded as minor the operator must show evidence of intended measures to be undertaken to reduce the number of errors occurring in his customs transactions.
The following checklist may assist customs officers when evaluating whether an infringement could be regarded as minor:

- It is recommended that infringements are looked at on a cumulative basis;
- The frequency of the infringement should be examined in relation to the number and size of the customs related operations;
- There must be no deliberate fraud intended;
- Context should always be considered;
- If the operator's agent is responsible for the infringements, then the operator must show evidence of intended measures to be undertaken by him to reduce the number of infringements by his agent.

Note: The information of the two following sub-sections can mainly be gathered by the customs authority itself, on the basis of information from various sources within the customs authority including national and international enforcement agencies.

I.2.2.1 Subsection 1 Compliance history as regards customs authorities and other relevant governmental authorities

2.01.	Indicator	Risk description	Points for attention	
1.	Customs transactions	Irregularities in combination with a high volume of business can result in a high financial or non-financial risk.	• Total number of customs declarations over the last 3 years by type. Any substantial changes expected in the coming years. • Customs offices involved. • Overview of the custom brokers/ agents (names, address, and number) involved.	
2.	Compliance check[20]	Non-compliant behaviour	Was the result of the last compliance check positive? If no, which measures has the applicant taken to avoid non-compliant behavior?	
3.	(Former) Applications for authorisations	Non-compliant behaviour	Specify whether, in the last three years, a customs authorisation in the applicant's name has been revoked, suspended or whether an application for a customs authorisation did not lead to the issuing of a license, and if so what was the motivation of the customs authority.	
4.	Customs compliance	Inadequate awareness of breaches against customs rules.	Has the applicant established procedures on disclosing irregularities to the relevant governmental agencies? Describe the routines for handing over information to Customs where criminal activity is suspected?	

I.2.1.2 Subsection 2 Intelligence information

2.02.	Indicator	Risk description	Points for attention	
1.	Irregularities	Non-compliant behaviour	a) Specify any fiscal and non-fiscal irregularities as regards customs law and procedures as well as other relevant legislative obligations in respect of the import, export and transport of goods. b) Has the applicant been the subject of anti-fraud investigations? c) Is the applicant handling in specific high risk goods such as weapons, dual-use goods, excise goods or CAP goods?	

I.2.3 Section III The applicants accounting and logistical system

Criterion:

A satisfactory system of managing commercial and where appropriate, transport records, which allow appropriate customs controls
Article 14i of CCIP

The following sub-section corresponds to the following sub-criteria:

Article 14i (a) of CCIP: The applicant shall maintain an accounting system which is consistent with the generally accepted accounting principles applied in the Member State where the accounts are held and which will facilitate audit-based customs control.

Article 14i (b) of CCIP: To enable the customs authorities to apply the necessary controls, the applicant has to allow the customs authority physical or electronic access to the customs and, where appropriate, transport records. Electronic access is not a pre-requisite to comply with this requirement.

Article 14i (c) of CCIP: The applicant shall have a logistical system which distinguishes between Community and non-Community goods, the fulfilment of this criterion is not needed in the case of an AEO Certificate - Security and Safety. This requirement is not applicable to AEO – Security and Safety.

Access to company's records

Access to a company's records is defined as the possibility of getting the required information, no matter where the data is physically stored. Required information includes company's records as well as other relevant information, which is needed to perform the pre-audit.
Access can take place in different ways:

- **Paper-based:** a hard copy of the required information is handed out. Paper-based solution is suitable when the quantity of the required information is limited. This situation can for instance occur when annual accounts are checked.
- **CD_ROM etc**: a copy of the required information is handed out as a CD-ROM or the like. The situation is appropriate when bigger quantity of information is involved and data processing is needed. The situation can for instance occur when all or an extract of financial transactions of a specific supplier account is checked in a given period of time.
- **"On-line access":** through the company computer system in case of site visit. The situation is a mixture of the two above-mentioned cases.

No matter which way data is accessible, customs authorities should have the possibility of data processing (e.g. is able to work on the data).

I.2.3.1 Subsection 1 Audit trail

In accounting, an audit trail is a process or an instance of cross-referring each bookkeeping entry to its source in order to facilitate checking its accuracy. A complete audit trail will enable to track the lifecycle of operational activities, in this respect related to the flow of goods and products coming in, being processed and leaving the applicant. Many businesses and organizations require an audit trail in their automated systems for security reasons. The audit trail maintains a historical record of the data that enables you to trace a piece of data from the moment it enters the data file to the time it leaves.

3.01.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Level of access for competent authorities	▪ Inability to readily undertake an audit due to the way in which the applicant's accounting system is structured. ▪ Lack of the control over the system's security and access.	a) Customs authorities shall have access to the applicant's records for control purposes including summary declarations, as required. b) Are an audit trail for fiscal and/or customs purposes available?	ISO 9001:2001, section 6.3

I.2.3.2 Subsection 2 Accounting system

3.02.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Computerised environment	Complex management system offers possibilities to cover-up illegal transactions. Omission of the connection between the flow of goods and the flow of money.	Organisation of the applicant's computerised environment. The following elements should be included: - The extent of the computerisation on the basis of the following scale: mainframe /mini/PC network or stand-alone PC. - The hardware platform available and the operating system running on it. - The separation of functions (between development, testing and operations) within the computer department (functions) organised. - The separation of functions between users and computerisation organised. - The separation of functions among users organised in the system. - How is access to the various parts of the system controlled? - Which applications have been accommodated elsewhere? - To which software house have these been assigned?	ISO 9001:2001, section 6.3

3.02.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
2.	Integrated accounting system	Incorrect and/or incomplete recording of transactions in the accounting system. Lack of segregation of duties between functions.[21] Lack of reconciliation between stock and accounting records.	Are the financial accounts and the logistical accounts part of one integrated accounting system? **Financial administration** Give an outline description of the financial system. Incorporate the following elements in your description or in the answer to the following questions: a) Specify which software package your company uses. b) Is this a bespoke or a standard package? c) Who is the manufacturer/supplier of the package? d) Have any adaptations been made to the standard package. If so, what adaptations have been made and for what reason? e) Where and by whom is the financial administration carried out? f) Give a list of the ledger accounts that are used. g) Who checks whether the entries in the sub-administration match those in the ledger? h) Does the system make use of verification interim accounts? Who is responsible for the co-ordination of these verification interim accounts? If so, give an overview of the ledger accounts with descriptions of where this registration takes place. i) Are the liabilities to import duty/excise recorded in the ledger in an intra-accountable manner? If so, give an	

[21] Segregation of duties should be examined in close correlation with the size of the applicant. For example, a micro-enterprise which is performing road transport business with small amount of everyday operations: packing, handling, loading/unloading of goods might be assigned to the driver of the truck. The receipt of the goods, their entering in the administration system and the payment/receipt of invoices should be assigned however to another person(s).

3.02.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
			overview of the ledger accounts with descriptions of where this record takes place. j) Can non-community goods suppliers be distinguished from community goods suppliers? **Logistical administration** a) Which software package the applicant is using? b) Is this an in-house or a standard package? c) Who is the manufacturer/supplier of the package? d) Have any adaptations been made to the standard package. If so, what adaptations have been made and for what reason. e) Where and by whom is the logistical administration carried out? f) Is there a separation between the office stock and the warehouse stock administration? g) Do you operate in batches? h) Is the stock administration linked up with the financial administration in an automated fashion? If not, what is the interface between the stock administration and the financial administration? i) How can the non-community goods or goods subject to customs control in the logistical administration be distinguished from the community goods	

Criterion:

A satisfactory system of managing commercial and where appropriate, transport records, which allow appropriate customs controls

Article 14i (d) of CCIP: The applicant shall have an administrative organisation which corresponds to the type and size of business and which is suitable for the management of the flow of goods, and have internal controls capable of detecting illegal or irregular transactions.

Article 14i (e) of CCIP: The applicant shall have, where applicable satisfactory procedures in place for the handling of licenses and authorisations connected to commercial policy measures or to the trade in agricultural products.

I.2.3.3 Subsection 3 Internal control system

3.03.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Internal control procedures	▪ Incorrect and/or incomplete recording of transactions in the accounting system. ▪ The use of incorrect or outdated standing data, such as article numbers and tariff codes.	a) Have guidelines been issued within the company by the board of directors, which employees within the purchase, storage, production and sale processes as well as transportation and freight forwarding must abide by. If so, have these guidelines been registered? b) Give an overview of the guidelines laid down. c) Does the company use any standards related to the accounting systems? d) Are guidelines regularly updated and reviewed? **Internal assessment** a) Describe in outline the internal procedures which are aimed at assessing the existence and operation of the administrative organisation and internal controls (henceforth: AO/IC) in relation to the flow of goods. If findings have been reported in the framework of this assessment in the last three financial years, provide an overview of those findings and of the measures that have been taken to improve matters. **Standing data** a) Describe the procedures concerning the change of	ISO 9001:2001, subsection. 7.4

3.03.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
			standing data (master files) which are relevant for customs (for instance standing files of creditors, article numbers, commodity codes and statistical numbers). b) Who/which department(s) is (are) responsible for these? c) In what way are adjustments archived? d) In what way are permanent (standing) data stored in digital form? e) Is a record being kept of permanent (standing) data?	
2.	Internal control procedures specifically for production	▪ Inadequate control within the applicant over the business processes. ▪ No or weak internal control procedures offer possibilities for fraud, unauthorized or illegal activities.	a) Is the production function separate from the purchase function, the sale function and the administration? b) Who/which department performs the re-calculation and on the basis of what data? c) Is there-calculation drawn up for each period or for each production run? d) Describe the discrepancy settlement procedure regarding the pre- and re-calculation. By whom is this carried out? e) Who enters what data in the supply and financial administration in relation to the supplies, which have been deployed in the production process? On what basis are these carried out? f) In what way are production results processed in the financial administration? g) What kind of journal entries does the production process give rise to?	ISO 9001:2001, sections 5.5, 6.3, 7.5, 8.2, 8.5

I.2.3.4 Subsection 4 Flow of goods

If necessary for reasons of clarity, a flow chart can be made up to visualise flows of goods. Also, existing flowcharts drawn up by the applicant can be used for this purpose.

3.04.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	General	Lack of control over stock movements offers possibilities to add dangerous and/or terrorist related goods to the stock and to take goods out of stock without appropriate registration.	a) Are internal goods movements recorded and are the connections between the different steps in these internal goods movements established? If so, with what frequency and by whom? b) Is this done in quantities and/or in money? c) Who analyses these goods movements and how often? d) Who authorizes the processing of the deviations established? e) Which standards are being applied in this connection?	ISO 9001:2001, section 6.3
2.	Incoming flow of goods	▪ Lack of reconciliation between goods ordered, goods received and entries to accounting records. ▪ Lack of control over stock movements offers possibilities to add dangerous and/or terrorist related goods to the stock and to take goods out of stock without appropriate registration.	a) Purchase and receipt procedures for goods imported from non-Community Countries. b) How (on the basis of which documents), when and by whom are imported goods entered in the stock administration system? c) At which point in time is the entry booked in the stock? d) Accounting systems associated with purchasing, receipt and payment of goods e) Arrangements for returning goods. f) Arrangements for intake deviations. g) Arrangements for incorrect entries in the stock administration. h) Details of inventory procedures.	ISO 9001:2001, section 6.3

3.04.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
3.	Storage	▪ Lack of control over stock movements. ▪ Lack of control over stock movements offers possibilities to add dangerous and/or terrorist related goods to the stock and to take goods out of stock without appropriate registration.	a) Does the applicant have appropriate procedures in place to control the goods in stock? Such procedures can – amongst others – be comprised of the following measures: ✓ a clear assignment of a location for storage of the goods; ✓ existence of a stock-taking procedure; ✓ procedures in case a temporary location is chosen to store the goods; ✓ arrangements for controlling breakage, decay or destruction of goods.	ISO 9001:2001, section 6.3
4.	Production	▪ Lack of control over stock used in the manufacturing process. ▪ Lack of control over stock movements offers possibilities to add dangerous and/or terrorist related goods to the stock and to take goods out of stock without appropriate registration.	Identify if the applicant has appropriate procedures in place to control the manufacturing processes. a) Describe the procedure as regards the request for raw materials and the delivery from the warehouse. b) Describe the procedure as regards logging the use of the raw materials in the production process. c) Describe the procedure as regards the registering of the finished manufactured product. d) Describe the procedure as regards losses in the production process. e) Describe the procedure as regards the release of the finished product to the warehouse. Such procedures can – amongst others - be comprised of the following measures: - Department which is responsible for the assignment for production. - The people responsible for the assignment for	ISO 9001:2001, section 6.3

3.04.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
			production register this in the administration. - Use of standard manufacturing methods in the production. - Appropriate documentation of the manufacturing methods. - Regular control of the manufacturing methods. - End products should be subjected to a quality inspection. - Inspection results should be registered.	
5.	Outgoing flow of goods Delivery from warehouse and shipment and transfer of goods	▪ Lack of control over stock movements offers possibilities to add dangerous and/or terrorist related goods to the stock and to take goods out of stock without appropriate registration. ▪ Lack of reconciliation between stock records and entries to the accounting records. ▪ Failure to make appropriate voluntary disclosures.	Identify if the applicant has appropriate procedures in place to control the release of goods from the warehouse and the shipment of goods. Such procedures can – amongst others – be comprised of the following measures: ✓ Sales department informs – on the basis of standardized procedures - the warehouse of the sale order/release of the goods. ✓ Persons are appointed as authorized to decide if the goods are ready for sale/release. ✓ Release of the goods is appropriately registered. ✓ A standardized information procedure between the warehouse keeper and the applicant's unit/department responsible for customs matters, to enable internal synchronization of the delivery of goods and starting of the export procedure. ✓ A final check before release to compare the order of release against the goods which are loaded. ✓ Standard operating procedures for returned goods – inspection, counting and registering.	ISO 9001:2001, sections 6.3, 7.1

I.2.3.5 Subsection 5 Customs routines

3.05.	Indicator	Risk description	Points for attention	
1.	General	Ineligible use of the routines	Describe the details of handling routines of customs declarations. In case of manufacturers, exporters, warehouse keepers and importers there should be internal procedures to verify customs transactions conducted by direct and or indirect representatives.	ISO 9001:2001, section 6.2.2
2.	Licences for import and/or export connected to commercial policy measures or to trade in agricultural goods	Ineligible use of goods	Identify if the applicant trades in goods that are subject to economic trade licences (for example, textiles sector). If that is the case there should be appropriate routines and procedures in place for administering the licences related to the import and/or export of goods.Such procedures can – amongst others – be comprised of the following measures: ✓ Registration of the licences on the basis of standard procedures. ✓ Regular control of the licences on validity and registration. ✓ Registration of the licences is done by a separate person or a group of persons than the control of the licenses. ✓ Standards for reporting irregularities with the licences ✓ Procedures to control the use of the goods to which the licences relate.	

A satisfactory system of managing commercial and where appropriate, transport records, which allow appropriate customs controls

Article 14i (f) of CCIP: The applicant shall have satisfactory procedures in place for the archiving of the applicant's records and information and for protection against the loss of information.

Article 14i (g) of CCIP: The applicant shall ensure that employees are made aware of the need to inform the customs authorities whenever compliance difficulties are discovered and establish suitable contacts to inform the customs authorities of such occurrences; (for example: unusual or suspicious cargo documentation; abnormal requests for information on shipments; unaccounted for cargo; compromised seals etc.).

Article 14i (h) of CCIP: The applicant shall have appropriate information technology security measures – for example firewalls and anti-virus protection - to protect the applicant's computer system from unauthorised intrusion and to secure the applicant's documentation.

I.2.3.6 Subsection 6 Procedures as regards back-up, recovery and fall-back and archival options

3.06	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Requirements for record keeping /archiving	▪ Inability to readily undertake an audit due to the way in which the applicant's accounting system is structured. ▪ Deliberate destruction or lost of relevant information	Give a description of procedures regarding back-up, recovery and fall-back option, taking account of the following questions, where applicable. ✓ How long does data remain available on-line, in its original form? ✓ How long does data remain accessible on-line, and how long does it remain available for an archive/history or statistical summary. ✓ How long is data kept on record off-line? ✓ On what kind of media is data stored. ✓ In which (software) format is data stored. ✓ Does data get compressed and at what stage. ✓ What are the guarantees as regards the long-term availability (technical quality of the recording media, availability of the hardware and program code, descriptions of the data and the program code)	ISO 9001:2001, section 6.3 ISO 17799:2005 ISO 27001:2005 ISO norms for standards in the IT security

I.2.3.7 Subsection 7 Information security – protection of computer systems

3.07	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Certification standards for securing computerised environment	Unauthorized access and/or intrusion to the economic operator's computer systems.	Are any existing certification standards applied for securing computer systems?	ISO 17799:2005 ISO 27001:2005
2.	Internal control procedures	▪ Unauthorized access and/or intrusion to the economic operator's computer systems. ▪ Deliberate destruction or lost of relevant information.	a) What measures are in place (for example: firewall; periodically changed passwords) to protect the economic operators' computer systems against unauthorized intrusion? b) Has any intrusion test been made? If no, the applicant should do these tests to show the security of their system. Such procedures can – amongst others – be comprised of the following measures: ✓ An updated, documented policy on protection of the applicant's computer systems; registered access for authorized persons; regular change of passwords; monitoring systems etc. An updated safety plan describing the measures in place protecting computer systems from unauthorised access as well as deliberate destruction or lost of information.	ISO/PAS 28001:2006, section A 3.3 ISO 27001:2005
3.	Computerised environment	▪ Unauthorized access and/or intrusion to the economic operator's computer systems. ▪ Deliberate	a) What policy/procedures exist for issuing authorizations for access and the level of access to the computer systems? Access to sensitive information should be limited to the staff members who are authorized to apply changes and additions to the information. b) Who is responsible for the protection and running of	ISO/PAS 28001:2006, section A 3.3 ISO 27001:2005

3.07	Indicator	Risk description	Points for attention	Possible references to international recognized standards
		destruction or lost of relevant information.	the applicant's computer system? Responsibility should not be limited to one person only but to several persons who are able to monitor each others actions.	
4.	Contingency plan	▪ Unauthorized access and/or intrusion to the economic operator's computer systems. ▪ Deliberate destruction or lost of relevant information.	The applicant should have an action plan with procedures in case of incidents.	ISO/PAS 28001:2006, section A 3.3 ISO 27001:2005
5.	Routines in case of computer failure	▪ Unauthorized access and/or intrusion to the economic operator's computer systems. ▪ Deliberate destruction or lost of relevant information.	The applicant should have back-up routines when computer systems don't work. There should also be procedures on bringing the information in the computer systems when they operate again.	ISO 27001:2005

I.2.3.8 Subsection 8 Information security – documentation security

3.08.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Internal control procedures	▪ Misuse of the economic operator's information system to endanger the supply chain. ▪ Deliberate destruction or lost of relevant information.	a) What measures are in place to protect the economic operators' documentation against unauthorized intrusion? b) Has any intrusion test been made with positive results? If no, the applicant should do these tests to show the security of their system. Such procedures can – amongst others – be comprised of the following measures: ✓ An updated, documented policy on documentation security: registration methods of document, access authorisations, back-up of documents etc. ✓ An updated safety plan describing the measures in place protecting documents from unauthorised access as well as deliberate destruction or lost of documents. ✓ Procedures on filing and storage of documents.	ISO/PAS 28001:2006, section A 4.2 ISO 17799:2005 ISO 27001:2005
2.	Contingency plan	▪ Misuse of the economic operator's information system to endanger the supply chain. ▪ Deliberate destruction or lost of relevant information.	Identify if during the last year incidents have occurred and what type of measures have been taken as a result thereof to improve the information/documentation security;	

3.	Authorisation level for staff categories	▪ Misuse of the economic operator's information system to endanger the supply chain. ▪ Deliberate destruction or lost of relevant information.	Which staff categories have access to particulars concerning goods and information flows? Which staff categories are authorised to change these particulars?	ISO/PAS 28001:2006, section A 3.3
4.	Safety and security requirements imposed on others	▪ Misuse of the economic operator's information system to endanger the supply chain. ▪ Deliberate destruction or lost of relevant information.	What security requirements have you placed on your trade partners and other contacts handling sensitive information provided by you?	

I.2.4 Section IV Financial solvency

Criterion:
Proven financial solvency
Article 14j of CCIP

As indicated in Article 14j of CCIP, the condition relating to the financial solvency of the applicant shall be deemed to be met if his solvency can be proven for the past three years. The legislation lays down that financial solvency means a good financial standing which is sufficient to fulfil the commitments of the applicant, with due regard to the characteristics of the type of the business activity.

If the applicant has been established for less then three years, his financial solvency shall be judged on the basis of records and information that are available.

It is recognised in some circumstances that it may be normal practice for a business to have negative net assets, for example when a company is set up by a parent company for research and development purposes when the liabilities may be funded by a loan from the parent or a financial institution. In these circumstances negative net assets may not be an indicator that a business is unable to pay their legal debts. However, the customs authority may require further evidence such as an undertaking from the lender or a bank facilities letter to satisfy the requirement or, if the company is a sole proprietor or for example a partnership, a list of any personal assets that are used to support the solvency of the business.

There are many possibilities to check whether the applicant meets this criterion. The depth of information-gathering is also subject to the issue whether the applicant is a known client of the customs authority.

- Customs authorities may check and analyse the balance and financial movements of the applicant in order to analyse the applicant's ability to pay their legal debts.
- In most cases the banking relation of the applicant will be able to report on his financial solvency.
- National central bank or other financial institutions of the applicant can also be solicited (statements, reports or evidences of any kind).
- Credit protection associations can be consulted if needed.
- Proof of the financial solvency could also be provided by the applicant itself. For example, the applicant could make reference to an audit report, to it’s ranking by a bank, or to information from a bank. These documents can then be inspected during the audit.

Further on, customs authorities can also establish whether the applicant is able to pay its legal debts by checking:

- **The applicant is not listed currently in insolvency or liquidation.**
- **The applicant has not entered into a current time to pay agreement. (Agreements made between an economic operator and customs authorities for the operator to pay their debts to customs authorities over an agreed period of time, if they are in financial difficulty or have cash flow problems and are therefore unable to pay the debt at the due date).**
- **The applicant did not have a bailiff visit or claim against its duty deferment guarantee in the last three years.**
- **The applicant was not late in paying money that is legally due to customs in the last three years (this excludes amounts that are not yet legally due or are under appeal).**

Information, whether the applicant is able to pay its debts to *third parties*, can also provide useful background for a decision. Customs authorities could examine the applicant's full sets of annual accounts due in the last three years and take into account:

- **Where required by company law, the accounts have been filed within the time limits laid down in that law.**
- **Comments about the continuation of the business as a going concern by for example the auditors or directors.**
- **The net current assets position.**
- **The net assets position and the extent intangible assets are included.**

Notice related to SME:
It is not unusual for a small company sometimes to apply for payment facilities as provided for in Article 229 of the Code. The existence of such isolated deferral applications should not result automatically in the applicant then being regarded as being unable to pay, and thus being denied the AEO status.

Notice related to parent company/subsidiaries:
When judging the financial situation of a subsidiary, it should be taken into account that a subsidiary company may operate under a guarantee from the parent company. Customs authorities may request further evidence in connection with the undertaking of the guarantor.

Notice related to newly established business:
Its financial solvency will be judged, according to Article 14j (2) of CCIP, on the basis of records and information that are available at the time of the application. This could include the latest cash flow, balance sheet and profit and loss forecasts approved by the directors/partners/sole proprietor. If the applicant's business is financed by a loan from another person or financial institution, the customs authority can also require a copy of the applicant's business case, the bank facilities letter and evidence the applicant is operating within its approved overdraft facility.

Notice related to insolvency or recovery proceedings:
In case the operator is subject to any insolvency or recovery proceeding, information should be gathered on the circumstances which have led to the initiation of the proceedings (economic recession, collapse of subsidiaries, temporary and unexpected changes in market trends), as well as on the amounts due. The amounts due can be compared with to the amount of different types of assets property of the applicant, i.e., current assets (cash and other liquid instruments, including accounts receivable, that can be converted to cash within one year at maximum), long term assets (plants, equipment, real estate and other capital assets, net of depreciation), intangible assets (assets with a determined value, but which may not be scalable, such as goodwill, patents, copyrights, and brand name recognition) and prepaid and deferred assets (expenditures for future costs or expenses, such as insurance, interest or rent, that are set up as assets to be amortized over an applicable period). It has to be analysed if the insolvency can effect in a negative way the compliance of the applicant and its business processes (wherever possible, identification of the main creditors and determination if they are subject to security and customs risk).

The term of "insolvency" within the meaning of these AEO Guidelines is recommended not to be regarded as an equivalent to "bankruptcy" which means a legally declared, usually by a court, inability or impairment of ability of a company to pay their creditors. Creditors may file bankruptcy for a debtor in an effort to recoup a portion of what they are owed. In the majority of cases, bankruptcy is initiated by the debtor (the bankrupt company). Pursuant to Article 14f of CCIP, an AEO application must be rejected because of bankruptcy, this rejection should have been notified before the customs authority starts the audit.

I.2.4.1 Subsection 1 Insolvency

4.01.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Insolvency	Non-compliant behaviour	Check and analyse the balance and financial movements of the applicant to analyse the applicant's ability to pay their legal debts. In most cases the banking relation of the applicant will be able to report on the financial solvency of the applicant.	

I.2.5 Section V Safety and security requirements

Criterion:
Appropriate security and safety standards
Article 14k (1) of CCIP

I.2.5.1 Subsection 1 Security assessment conducted by the economic operator (self assessment)

The operator should demonstrate in its policy a high-level of awareness on security and safety measures, internally and in its business activities with clients, suppliers and external service providers. In preparation of the pre-audit of customs authorities the operator can do a self assessment to enable himself to analyse if he is able to meet the security requirements. The assessment is an attempt to identify the risks and threats which might occur in that part of the supply chain in which the applicant is operating, and to look into the measures in place to minimise the risks and threats. This area is not mentioned in the implementing provisions but should be seen as a help for the applicant to meet the security criteria. It is a working method mentioned in for example in AEO COMPACT model, ISO PAS 28001 and it is a mandatory requirement in the ISPS Code.

5.01.	Indicator	Risk description	Assessment questions	Possible references to international recognized standards
1.	Self assessment	Inadequate safety and security awareness	What kind of safety and security risks or dangers have you identified?	ISO/PAS 28001:2006, section A.4.2 ISPS Code
2.	Internal organisation	Inadequate coordination about safety and security within the applicant	How are safety and security measures coordinated within your applicant? Indicate which person and/or unit of your company is responsible for this coordination.	ISO/PAS 28001:2006, section A.3.3 ISO 9001:2001, section 5.5.1 ISPS Code
3.	Internal control system	Inadequate control within the applicant over safety and security issues	Are there any existing documented security routines and how are they communicated to the personnel and other people visiting your company?	ISO/PAS 28001:2006, section A.3.3, A.4.2 ISPS Code
4.	Internal control procedures	Incorrect and/or incomplete registration of safety and security incidents. Absence of appropriate countermeasures to safety and security incidents.	During the last year what type of incidents have occurred and what type of measures have resulted thereof? Does the threat assessment cover these types of incidents or not? What procedures exist for registering and reporting of incidents?	ISO/PAS 28001:2006, section A.3.3, A.4.2 ISPS Code

5.	Certification for safety and security purposes by others	Inadequate safety and security measures	Have you already been certified by another public agency or public body for (transport) security purposes?	ISO/PAS 28001:2006, section A.3.3, A.4.3 ISPS Code **Recognized security certificates for maritime traffic stakeholders : ISPS code agreement as referred to in Regulation (EC) No 725 /2004 of European Parliament and of the Council** **Recognized security certificates for air traffic stakeholders as referred to in Regulation (EC) No 2320/2002 of European Parliament and of the Council and in Regulation (EC) No 622/2003** When homologed, ISO/PAS standard 28001 related to Security management systems for the international supply chain.
6.	Safety and security requirements specific to goods	Inadequate implementation of safety and security requirements	Are there particular security and safety requirements for the goods you are importing/exporting?	ISPS Code
7.	Threat assessment by others	Inadequate safety and security awareness	If you are making use of the services of a security company; has this company made a threat assessment of your company?	ISPS Code
8.	Security requirements imposed by others	Inadequate safety and security measures	Does your insurance company impose security requirements on you? Have your customers imposed security arrangements on you?	ISPS Code

Criterion:
Appropriate security and safety standards:

Article 14k (1) (a) of CCIP: The area shall be considered to be appropriate if buildings to be used in connection with the operations to be covered by the certificate are constructed of materials, which resist unlawful entry and provide protection against unlawful intrusion;

Article 14k (a) (b) of CCIP: Appropriate access control measures are in place to prevent unauthorised access to shipping areas, loading docks and cargo areas.

I.2.5.2 Subsection 2 Entry and access to premises

5.02.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Routines for access or entry of vehicles, persons and goods	Unauthorized access or entry of vehicles, persons or goods to the premises and/or close to the loading and shipping area.	Identify the access control system in place. Only properly identified and authorized persons, vehicles and goods are permitted to access the premises. Access to premises should be controlled. Persons should use badges. The badges should be issued and supervised by the applicant.	ISO/PAS 28001:2006, section A.3.3 ISPS Code
2.	Standard operating procedures in case of intrusion	No proper action if intrusion has been discovered.	The applicant should have established procedures to respond when an unauthorized intruder has been discovered on the premises (e.g. contact local policy authority, involvement of internal security staff).	ISO/PAS 28001:2006, section A.3.3 ISPS Code

I.2.5.3 Subsection 3 Physical security

5.03.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	External boundaries of premises	Inadequate protection of the premises against external intrusion.	How are the external boundaries of the premises secured? All buildings should be constructed of materials which resist unlawful entry and protect against external intrusion. All external and internal windows, gates and fences must be secured with locking devices or alternative access monitoring or control measures such as internal/external anti-burglar alarm systems or CCTV (close circuit TV systems)	ISO/PAS 28001:2006, section A.3.3 ISPS Code
2.	Gates and gateways	Existence of gates or gateways which are not monitored.	Identify all gates or gateways at the premises. When the gates or gateways are not locked they should be manned or guarded with alternative access monitoring or control measures.	ISO/PAS 28001:2006, section A.3.3 ISPS Code
3.	Locking devices	Inadequate locking devices for external and internal doors, windows, gates and fences.	What kinds of locks are inner and outer doors, windows and gates equipped with?	ISO/PAS 28001:2006, section A.3.3
4.	Lighting	Inadequate lighting for external and internal doors, windows, gates, fences and parking areas	Where appropriate, adequate lighting should be provided.	

5.03.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
5.	Procedures for access to keys	Unauthorized access to keys.	There should exist procedures for access to the keys. Only a limited number of persons should be authorised to have access to the keys. Keys should be kept in a specially appointed place. A person should be kept responsible for the keys. There should exist a method of registering of who is using the keys when they were taken and by whom and when they are brought back to the appointed place.	ISO/PAS 28001:2006, section A.3.3
6.	Internal physical security measures	Inappropriate access to internal sections of the premises.	Are there internal physical security measures? Only properly identified and authorized persons should have access to internal sections of the premises.	ISO/PAS 28001:2006, section A.3.3, A.4.2 ISPS Code
7.	Parking of private vehicles	Inadequate protection of the premises against external intrusion	The applicant should have monitoring procedures in place to avoid parking of private vehicles close to secured areas of the premises.	
8.	Maintenance external boundaries and buildings	Inappropriate maintenance of the external boundaries of the premises and the buildings.	The external boundaries and buildings should be regularly checked either by a specially appointed person or by a third party. If a third party is responsible for checking and maintenance of the external boundaries and buildings, they have to report to staff member of the applicant who is appointed for controlling maintenance works on the external boundaries and buildings.	ISO/PAS 28001:2006, section A.3.3

Criterion:

***Appropriate security and safety standards**:*

Article 14k (1) (c) of CCIP: The area shall be considered to be appropriate if measures for the handling of goods include protection against the introduction, exchange or loss of any material and tampering with cargo units;

Article 14k (1) (d) of CCIP: Where applicable, procedures are in place for the handling of import and/or export licenses connected to prohibitions and restrictions and to distinguish these goods from other goods.

I.2.5.4 Subsection 4 Cargo units

5.04.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Routines for access to cargo units	Unauthorized access to cargo units.	Only properly identified and authorized persons should have access to the cargo units.	ISO/PAS 28001:2006, section A.3.3 ISPS Code
2.	Routines for ensuring the integrity of cargo units	Tampering with cargo units.	The integrity of cargo units should be ensured by placing them under permanent monitoring or keeping them in a safe, locked area.	ISO/PAS 28001:2006, section A.3.3 ISPS Code
3.	Use of seals	Tampering with cargo.	The AEO applicant should use – to the extent possible – seals that meet or are equivalent to the existing ISO standards. International agreements may set down specific standards for seals.	ISO/PAS 17712

5.04.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
4.	Procedures for inspecting the structure of the cargo unit	Use of hidden places in cargo units for smuggling purposes.	When appropriate to the type of cargo unit used a seven-point inspection process is recommended: o Front wall o Left side o Right side o Floor o Ceiling/Roof o Inside/outside doors o Outside/undercarriage	ISO/PAS 28001:2006, section A.3.3
5.	Standard operating procedures in case of intrusion and/or tampering with cargo units	No proper action if unauthorized access or tampering has been discovered.	The applicant should have appropriate procedures laid down on what measures should be taken when an unauthorized access or tampering is discovered.	ISO/PAS 28001:2006, section A.3.3
6.	Ownership of cargo units	To have incomplete control of the cargo units.	Does the applicant have ownership of the cargo units? If the applicant does not have ownership of the cargo units, procedures should be in place to examine the integrity of the cargo unit before loading. The inspection process mentioned under 5.04.3 should be mandatory for personnel.	
7.	Maintenance of cargo units	Tampering with cargo units.	Is the maintenance of the cargo units done at the premises or externally? Maintenance should be done routinely not only in case of damage or incidents. If the maintenance is done externally or not under supervision of companies staff the cargo unit's integrity should be inspected when returning to the applicant.	ISO/PAS 28001:2006, section A.3.3

I.2.5.5 Subsection5 Logistical processes

5.05.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Active means of transport	Lack of control over the transport of goods.	Identify which means of transport are normally used by the applicant. In case of manufacturers, exporters, warehouse keepers and importers indicate also if the transport is carried out by the applicant itself or external freight forwarders/carriers. If the latter is the case the applicant can use freight forwarders and/or carriers on a regular basis, there could be long-term contracts with freight forwarders and carriers. Identify if the freight forwarder or the carrier is member of a secure transport program, if not how the security is ensured. In the case of freight forwarders indicate if the transport is carried out by external carriers and if it is the case whether the external carriers are under long term contracts. In the case of carriers indicate whether he actually transports the goods or is in charge of or responsible for the operation of the means of transport.	

I.2.5.6 Subsection 6 Non-fiscal requirements

5.06.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Non-fiscal aspects	Ineligible use of goods	Does the applicant trade in goods that are subject to import and/or export licenses or special authorizations/licenses for trade connected to prohibitions and restrictions? Does the applicant trade in dual-use goods? Does the applicant trade in goods that are subject to an embargo? Where appropriate the applicant should establish routines: o to distinguish goods subject to non-fiscal requirements and other goods o to check if the operations are carried out in accordance with current (non-fiscal) legislation. o attached to the handling of goods subject to an embargo. o attached to the handling of licenses. o regarding other goods that are subject to restrictions. o to identify potential dual-use goods and routines attached to their handling.	

I.2.5.7 Subsection 7 Incoming goods

5.07.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Routines for checking incoming transport	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk.	Where appropriate the applicant should establish routines: o Appointing staff responsible of receiving the driver and the goods at arrival. o Registration of the transport documents and customs papers accompanying the goods. o Comparing the goods with the accompanying transport documents and customs papers. o Registration of the completion and results of the checks. o To inform the customs authorities informed on arrival of the goods to enable customs to perform controls of the shipments in time. o To inform the purchase department and the administration on the receipt of goods.	ISO 9001:2001, section 6.2.2 ISO/PAS 28001:2006, section A.3.3
2.	Routines for verifying security measures imposed on others	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk.	When there exist arrangements on security measures with domestic and foreign suppliers, staff should be aware of these arrangements and routines should be established to verify the commitments to these arrangements.	ISO/PAS 28001:2006, section A.3.3
3.	Supervision for the reception of goods	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk.	It should not be possible to deliver goods in an unsupervised area. The applicant should identify procedures avoiding the situation that goods are left unsupervised?	ISO/PAS 28001:2006, section A.3.3
4.	Level of safety and security awareness of personnel	Lack of proper knowledge on security with the consequence of accepting unsafe or insecure goods;	The applicant should on a regular basis inform the staff of security measures and/or security arrangements to ensure the safety and security awareness of personnel.	ISO/PAS 28001:2006, section A.3.3

5.07.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
		accepting goods which are not registered in a logistical system and of which you don't have any control.		
5.	Sealing of incoming goods	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk.	At reception of the goods, the integrity of seals should be checked. Where relevant the applicant should have routines to seal incoming goods.	ISO/PAS 28001:2006, section A.3.3 ISO/PAS 17712
6.	Uniform marking of goods	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk.	Incoming goods should be uniformly marked or stored in designated area(s).	ISO 9001:2000, section. 7.4
7.	Weighing and tallying of goods	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk.	Where relevant, the applicant should establish routines to weigh and tally incoming goods.	ISO 9001:2000, section. 7.4
8.	Administrative processes of the reception of goods	Lack of control of reception of goods which is not registered in a logistical system which might pose a safety or security risk.	The applicant should establish administrative procedures of the reception of goods: o How (on the basis of which documents), when and by whom are the goods received entered in the stock administration. o Checking of the goods against loading lists and purchase orders. o Registration of the goods in the stock, as soon as possible after arrival of the goods.	ISO 9001:2000, section. 7.4

5.07.	Indicator	Risk description	Questions	Possible references to international recognized standards
9.	Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	Internal control procedures should be in place when discrepancies and/or irregularities are discovered. There should exist a separation of functions between the ordering of the goods (purchase), receipt (warehouse), the entering of the goods in the system (administration) and the payment of the invoice.	

I.2.5.8 Subsection 8 Storage of goods

5.08.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Assignment of storage location	Inadequate protection of the storage area against external intrusion	An area or areas should be designated for the storage of goods	
2.	Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	There should be procedures in place concerning regular stocktaking. There should be procedures in place when discrepancies and/or irregularities are discovered.	ISO 9001:2001, section 2.2
3.	Separated storage of different goods	Unauthorized substitution of goods and/or tampering with goods.	Where appropriate different types of goods should be separated, e.g. foreign, domestic, high-value goods, hazardous goods etc (see also 5.06.1). The location of storage should be registered in the logistical administration, as soon as the goods are arrived in the storage location.	TAPA (Technology Asset Protection Association) Certificate
4.	Additional safety and security measures for access to goods	Unauthorized access to the goods.	Are there any security measures, additional to the ones mentioned in Sections 5.02 and 5.03, protecting the goods from access by unauthorized persons?	ISO/PAS 28001:2006, section A.3.3
5.	Authorisation level for staff categories	Unauthorized access to the goods.	Authorized access to the storage area and the goods only for designated staff or appropriately authorised persons.	ISO/PAS 28001:2006, section A.3.3 ISPS Code

I.2.5.9 Subsection 9 Production of goods

5.09.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Assignment of location	No full control over the production process.	An area or areas be designated for production of goods. When goods are produced externally, the applicant should have established security arrangements with the persons responsible for the external premises to ensure the integrity of the goods.	ISO/PAS 28001:2006, section A.3.3
2.	Internal control procedures	Tampering with the goods.	Security processes and procedures should be established to assure the integrity of the production process, e.g. authorized access only for designated staff or appropriately authorised persons, supervision and monitoring of the production process by systems and/or personnel. There should be a separation of functions between the person responsible for controlling the manufacturing methods and the person responsible to establish the manufacturing methods.	ISO/PAS 28001:2006, section A.3.3
3.	Additional safety and security measures for access to goods	Unauthorized access to the goods.	Are there any security measures, additional to the ones mentioned in Sections 5.02 and 5.03, protecting the goods from access by unauthorized persons?	ISO/PAS 28001:2006, section A.3.3
4.	Authorisation level for staff categories	Unauthorized access to the goods.	Authorized access to the production area only for designated staff or appropriately authorised persons.	ISO/PAS 28001:2006, section A.3.3
5.	Packing of products	Incomplete control over the flow of goods.	When the packing of final products is not done at the applicant's premises but externally, the applicant should have established security arrangements with the persons responsible for the external premises to ensure the integrity of the goods.	
6.	Quality inspection	Incomplete control over the flow of goods.	If a quality inspection exists for the goods, which can be an additional element to ensure the security integrity of the goods.	

I.2.5.10 Subsection 10 Loading of goods

5.10.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Routines for checking outgoing transport	Lack of control of delivery of goods which is not registered in a logistical system which might pose a safety or security risk.	Where appropriate the applicant should establish routines: o Appointing staff responsible of receiving the driver and the loading of the goods at arrival. o Registration of the transport documents and customs papers accompanying the goods. o Comparing the goods with the accompanying transport documents and customs papers. o Registration of the completion and results of the checks. o To inform the customs authorities informed on departure of the goods to enable customs to perform controls of the shipments in time. o To inform the selling department and the administration on the departure of goods.	ISO/PAS 28001:2006, section A.3.3
2.	Routines for verifying security measures imposed by others	Breach of agreed security arrangements with the risk of delivery of unsafe or insecure goods; delivery of goods which is not registered in a logistical system and of which you don't have any control.	Where appropriate, how the arrangements on security measures imposed by your customers are verified when the goods are loaded.	ISO/PAS 28001:2006, section A.3.3

5.10.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
3.	Supervision over loading of goods	Lack of supervision of loading of goods	Personnel should be assigned to supervise the loading of goods. It should be avoided that outgoing goods could be loaded or left behind in unsupervised. The applicant should identify procedures avoiding the situation that goods are left unsupervised.	ISO/PAS 28001:2006, section A.3.3
4.	Level of safety and security awareness of personnel	Lack of proper knowledge on security with the consequence of loading unsafe or insecure goods. Loading goods which are not registered in a logistical system and of which you don't have any control.	The applicant should on a regular basis inform the staff of security measures and/or security arrangements to ensure the safety and security awareness of personnel.	ISO/PAS 28001:2006, section A.3.3 ISPS Code
5.	Sealing of outgoing goods	Lack of control of sealing of goods	Are outgoing goods sealed and how are the seals checked?	ISO/PAS 28001:2006, section A.3.3 ISO/PAS 11712:116 ISO PAS 17712
6.	Uniform marking of goods	Lack of control of delivery of goods which is not registered in a logistical system which might pose a safety or security risk.	Outgoing goods should be uniformly marked or stored in designated area(s).	

5.10.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
7.	Weighing and tallying of goods	Delivery of goods that pose a safety or security risk. Delivery of goods which is not registered in a logistical system and of which you don't have any control.	Where appropriate, the applicant should establish routines to weigh and tally outgoing goods.	
8.	Administrative processes of the loading of goods	Delivery of goods that pose a safety or security risk. Delivery of goods which is not registered in a logistical system and of which you don't have any control.	The applicant should establish administrative procedures of the delivery of goods: o How (on the basis of which documents), when and by whom are the goods loaded booked out in the stock administration. o Checking of the goods against loading lists and selling orders. o Registration of the goods out of the stock, as soon as possible after departure of the goods.	
9.	Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	Procedures should be in place when discrepancies and/or irregularities are discovered.	ISO/PAS 28001:2006, section A.3.3

Criterion:
Appropriate security and safety standards:

Article 14k (1) (e) of CCIP: The area shall be considered to be appropriate if the applicant has implemented measures allowing a clear identification of his business partners in order to secure the international supply chain.

Economic operators can only be held responsible for their part of the supply chain, and for the goods which are under their custody. Through contractual arrangements between the applicant and his business partners can the security of the sequent parts of the supply chain be ensured. Shipments not, or only partial covered by security measures, will not be regarded as fully secure and will therefore not benefit from the maximum possible treatment regarding lower risk score.

I.2.5.11 Subsection 11 Security requirements business partners

5.11.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Security requirements imposed on others	Breach of agreed security arrangements with the risk of delivering unsafe or unsecured goods.	Identify and analyse the arrangements which are made regarding the implementation of security measures between the applicant and its business partners. To the extent practical for the relevant business model, security measures could be introduced in the contractual arrangements. The effectiveness of the security requirements implemented by your business partners should be regularly checked based on risk analysis.	ISO/PAS 28001:2006, section A.3.3
2.	External control procedures	Breach of agreed security arrangements with the risk of delivering unsafe or unsecured goods.	Have during the last year incidents occurred with regard to the arrangements as mentioned above? If yes, what types of measures have resulted as a consequence of the incidents which happened?	

Criterion:
Appropriate security and safety standards, where applicable:

Article 14k (1) (f) of CCIP: The area shall be considered to be appropriate if the applicant conducts, in so far as legislation permits, security screening on prospective employees working in security sensitive positions and carries out periodic background checks;

Article 14k (1) (g) of CCIP: The applicant ensures that their staffs concerned participate in security awareness programmes.

I.2.5.12 Subsection 12 Personnel security

5.12.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	Employment policy	Infiltration of staff that could compose a security risk.	The applicant's employment policy should take account of the applicant's security requirements.	ISO/PAS 28001:2006, section A.3.3
2.	Security checks on prospective employees	Infiltration of staff that could compose a security risk.	If national legislation allows, the applicant should perform backgrounds checks on the new employees working on security sensitive posts. These checks may also concerned existing employees coming from other departments not regarded as sensitive from a security point of view and moving to such posts. Security checks methods may comprise, before recruitment, inquiries based on undeniable and/or official elements of previous employment history and references. For high and/or critical security posts, police checks on both spent and unspent convictions could be required. Appointed employees could inform their employer of police caution/bail, pending court proceedings and/or convictions. They should also disclose of any other employment or any activity subject to any security risks.	ISO/PAS 28001:2006, section A.3.3

			When staff leave or are dismissed, strict measures have to be taken to ensure that physical or “virtual” intrusion is no longer possible (removal of computer access, return of security pass or badge).	
3.	Safety and security training	Inadequate awareness of security requirements.	The personnel concerned should receive appropriate training, as logically based on the business model of the applicant, with regard to the security and safety risks associated with movements of goods in the international trade supply chain. Such training could provide information on the security protocols, detection of intrusion/tampering and reporting of incidents, recognition of potential internal threats to security and protecting access controls. The expression "personnel concerned" may mean, according to the specific circumstances, security personnel, cargo-handling and cargo-documentation personnel, as well as employees in the shipping and receiving areas to the extent they are within the applicant's control.	ISO/PAS 28001:2006, section A.3.3
4.	Safety and security requirements for temporary personnel	Infiltration of staff that could compose a security risk.	The applicant should have security requirements in place regarding the use of temporary personnel.	ISO/PAS 28001:2006, section A.3.3

I.2.5.13 Subsection 13 External services

5.13.	Indicator	Risk description	Points for attention	Possible references to international recognized standards
1.	External services	Infiltration of staff that could compose a security risk.	In case that services are outsourced, i.e.; transportation, security guards, cleaning, maintenance; security demands should be incorporated in the contractual arrangements made with the external companies.	ISO/PAS 28001:2006, section A.3.3

PART 3

I.1. Table of criteria that apply to the different actors in the supply chain

The table below indicates which areas of the criteria apply to the different parties in the supply chain listed in Part 1 Section IV. The table is only an overview of the areas; the detailed criteria are explained above in the sections and sub-sections of Part 2.

In case an AEO applicant combines in his business process several of the functions mentioned in this table, the columns should be merged to establish a complete list of criteria which have to be fulfilled:

1) In the case of an exporter transporting his own goods (without making use of the services of any freight forwarder) the columns "exporter" and "carrier" should be merged.

2) In case a company organises the transportation of the goods on behalf of an exporter and also owns and uses vehicle of conveyance for the cargo, and acts on behalf of the exporter as a customs agent, the columns “freight forwarder”, “carrier” and “customs agent” should be merged.

3) In case a freight forwarder also operates a customs warehouse in which he stores the goods of his clients the columns “freight forwarder” and “warehouse keeper” should be merged

4) If a customs agent performs warehousing activities too, the columns “customs agent” and “warehouse keeper” should be merged.

The letters "CSF" in the table means:
C: AEO Certificate - Customs Simplifications
S: AEO Certificate – Security and Safety
F: AEO Certificate Customs Simplifications / Security and Safety

		Manufacturer	*Exporter*	*Freight Forwarder*	*Warehouse keeper*	*Customs agent*	*Carrier*	*Importer*
1.01	**Volume of business**							
1.01.1	Annual Turnover (general)	CSF	CSF	CSF	CSF	CSF	CSF	CSF
1.01.2	Profits and losses	CSF	CSF	CSF	CSF	CSF	CSF	CSF
1.01.3	Stock Capacity	CSF	CSF	1) CSF	CSF	CSF	1) CSF	CSF
1.01.4	Purchases (foreign trade).	CSF	CSF					CSF
1.01.5	Goods received in customs or fiscal warehouse				CSF			
1.01.6	Goods used in the production process	CSF						
1.01.7	Outcome of the production process	CSF						
1.01.8	Sales (foreign trade)	CSF	CSF					
1.01.9	Goods removed from customs or fiscal warehouse				CSF			
1.02	**Statistics on customs matters**							
1.02.1	Tariff classification	3)	CSF			CSF		CSF
1.02.2	% of import duties	3)				CSF		CSF
1.02.3	% of VAT	3)				CSF		CSF
1.02.4	% of excise	3)				CSF		CSF
1.02.5	CAP (duties and refunds)	3)	CSF			CSF		
1.02.6	Preferential measures	3)	CSF			CSF		CSF
1.02.7	Antidumping duties	3)				CSF		CSF
1.02.8	Origin / provenance of goods	3)				CSF		
1.02.9	Customs/VAT value	3)	1) CSF			CSF		CSF
2.01	**Compliance history**							
2.01.1	Customs transactions	CSF	CSF	CSF	CSF	CSF	CSF	CSF
2.01.2	Compliance check	CSF	CSF	CSF	CSF	CSF	CSF	CSF
2.01.3	(Former) Applications for authorisations	CSF	CSF	CSF	CSF	CSF	CSF	CSF
2.01.4	Customs compliance	CSF	CSF	CSF	CSF	CSF	CSF	CSF
2.02	Intelligence information	CSF	CSF	CSF	CSF	CSF	CSF	CSF
2.02.1	Irregularities	CSF	CSF	CSF	CSF	CSF	CSF	CSF

		Manufacturer	*Exporter*	*Freight Forwarder*	*Warehouse keeper*	*Customs Agent*	*Carrier*	*Importer*
3	**The Applicant's Accounting and logistical system**							
3.01	Audit trail	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.01.1	Level of access for competent authorities	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.02	**Accounting system**	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.02.1	Computerised environment	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.02.2	Integrated accounting system	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.03	**Internal control system**							
3.03.1	Internal control procedures	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.03.2	Internal control procedures specifically for production	CSF						
3.04	**Flow of goods**							
3.04.1	General	CSF	CSF		CSF			CSF
3.04.2	Incoming flow of goods	CSF	CSF		CSF			CSF
3.04.3	Storage	CSF	CSF		CSF			CSF
3.04.4	Production	CSF						
3.04.5	Outgoing flow of goods. Delivery from warehouse and shipment and transfer of goods	CSF	CSF		CSF			
3.05	**Customs routines**							
3.05.1	General	1) CSF	1) CSF	1) CSF	1) CSF	1) CSF	CSF	1) CSF
3.05.2	Licenses for import and/or export connected to commercial policy measures or to trade in agricultural goods	1) CSF	1) CSF	1) CSF	1) CSF	1) CSF	CSF	1) CSF
3.06	**Procedures as regards back-up, recovery and fall- back and archival options**							
3.06.1	Requirements for record keeping/archiving	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.07	**Information security - protection of computer systems**							

		Manufacturer	*Exporter*	*Freight Forwarder*	*Warehouse keeper*	*Customs Agent*	*Carrier*	*Importer*
3.07.1	Certification standards for securing computerised environment	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.07.2	Internal control procedures	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.07.3	Computerised environment	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.07.4	Contingency plan	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.07.5	Routines in case of computer failure	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.08	**Information security - documentation security**							
3.08.1	Internal control procedures	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.08.2	Contingency plan	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.08.3	Authorisation level for staff categories	CSF	CSF	CSF	CSF	CSF	CSF	CSF
3.08.4	Safety and security requirements imposed on others	CSF	CSF	CSF	CSF	CSF	CSF	CSF
Section IV	**Financial Solvency**							
4.01	Insolvency	CSF	CSF	CSF	CSF	CSF	CSF	CSF
Section V	**Safety and Security requirements**							
5.01	Security assessment conducted by the economic operator	SF	SF	SF	SF	SF	SF	SF
5.01.1	Self assessment	SF	SF	SF	SF	SF	SF	SF
5.01.2	Internal organisation	SF	SF	SF	SF	SF	SF	SF
5.01.3	Internal control system	SF	SF	SF	SF	SF	SF	SF
5.01.4	Internal control procedures	SF	SF	SF	SF	SF	SF	SF
5.01.5	Certification for safety and security purposes by others	SF	SF	SF	SF	SF	SF	SF
5.01.6	Safety and security requirements specific to goods	SF	SF	SF	SF	SF	SF	SF
5.01.7	Threat assessment by others	SF	SF	SF	SF	SF	SF	SF
5.01.8	Security requirements imposed by others	SF	SF	SF	SF	SF	SF	SF
5.02	**Entry and access to premises**	SF	SF	SF	SF	SF	SF	SF

		Manufacturer	*Exporter*	*Freight Forwarder*	*Warehouse keeper*	*Customs Agent*	*Carrier*	*Importer*
5.02.1	Routines for access or entry of vehicles, persons and goods	SF	SF	SF	SF	SF	SF	SF
5.02.2	Standard operating procedures in case of intrusion	SF	SF	SF	SF	SF	SF	SF
5.03	**Physical security**	SF	SF	SF	SF	SF	SF	SF
5.03.1	External boundaries of premises	SF	SF	SF	SF	SF	SF	SF
5.03.2	Gates and gateways	SF	SF	SF	SF	SF	SF	SF
5.03.3	Locking devices	SF	SF	SF	SF	SF	SF	SF
5.03.4	Lighting	SF	SF	SF	SF	SF	SF	SF
5.03.5	Procedures for access to keys	SF	SF	SF	SF	SF	SF	SF
5.03.6	Internal physical security measures	SF	SF	SF	SF	SF	SF	SF
5.03.7	Parking of private vehicles	SF	SF	SF	SF	SF	SF	SF
5.03.8	Maintenance of external boundaries and buildings	SF	SF	SF	SF	SF	SF	SF
5.04	**Cargo units**							
5.04.1	Routines for access to cargo units	SF	SF	SF	SF	SF	SF	SF
5.04.2	Routines for securing the integrity of cargo units	SF	SF	SF	SF	SF	SF	SF
5.04.3	Use of seals	SF	SF	SF	SF	SF	SF	SF
5.04.4	Procedures for inspecting the structure of the cargo unit	SF	SF	SF	SF	SF	SF	SF
5.04.4	Standard operating procedures in case of intrusion and/or tampering with cargo units	SF	SF	SF	SF	SF	SF	SF
5.04.5	Ownership of cargo units	SF	SF	SF	SF	SF	SF	SF
5.04.6	Maintenance of cargo units	SF	SF	SF	SF	SF	SF	SF
5.05	Logistical processes							
5.05.1	Active means of transport	SF	SF	SF	SF	SF	SF	SF
5.06	Non-fiscal requirements	SF	SF	SF	SF	SF	SF	SF
5.06.1	Non-fiscal aspects	SF	SF	SF	SF	SF	SF	SF
5.07	**Incoming goods**	SF	SF	SF	SF	SF	SF	SF
5.07.1	Routines for checking incoming transport	SF	SF	SF	SF	SF	SF	SF

		Manufacturer	*Exporter*	*Freight Forwarder*	*Warehouse keeper*	*Customs Agent*	*Carrier*	*Importer*
5.07.2	Routines for verifying security measures imposed on others	SF	SF	SF	SF	SF	SF	SF
5.07.3	Supervision for the reception of goods	SF	SF	SF	SF	SF	SF	SF
5.07.4	Level of safety and security awareness of personnel	SF	SF	SF	SF	SF	SF	SF
5.07.5	Sealing of incoming goods	SF	SF	SF	SF	SF	SF	SF
5.07.6	Uniform marking of goods	SF	SF	SF	SF	SF	SF	SF
5.07.7	Weighing and tallying of goods	SF	SF	SF	SF	SF	SF	SF
5.07.8	Administrative processes of the reception of goods	SF	SF	SF	SF	SF	SF	SF
5.07.9	Internal control procedures	SF	SF	SF	SF	SF	SF	SF
5.08	**Storage of goods**							
5.08.1	Assignment of storage location	SF	SF	1) SF	SF	SF	1) SF	2) SF
5.08.2	Internal control procedures	SF	SF	1) SF	SF	SF	1) SF	2) SF
5.08.3	Separated storage of different goods	SF	SF	1) SF	SF	SF	1) SF	2) SF
5.08.4	Additional safety and security measures for access to goods	SF	SF	1) SF	SF	SF	1) SF	2) SF
5.08.5	Authorisation level for staff categories	SF	SF	1) SF	SF	SF	1) SF	2) SF
5.09	**Production of goods**							
5.09.1	Assignment of location	SF						
5.09.2	Internal control procedures	SF						
5.09.3	Additional safety and security measures for access to goods	SF						
5.09.4	Authorisation level for staff categories	SF						
5.09.5	Packing of products	SF	1) SF					
5.09.6	Quality inspection	SF	1) SF					
5.10	**Loading of goods**							
5.10.1	Routines for checking outgoing transport	SF	SF	SF	SF	SF	SF	
5.10.2	Routines for verifying security measures imposed by others	SF	SF	SF	SF	SF	SF	SF
5.10.3	Supervision over loading of goods	SF	SF	SF	SF	SF	SF	SF

		Manufacturer	*Exporter*	*Freight Forwarder*	*Warehouse keeper*	*Customs Agent*	*Carrier*	*Importer*
5.10.4	Level of safety and security awareness of personnel	SF	SF	SF	SF	SF	SF	SF
5.10.5	Sealing of outgoing goods	SF	SF	SF	SF	SF	SF	
5.10.6	Uniform marking of goods	SF	SF	SF	SF	SF	SF	SF
5.10.7	Weighing and tallying of goods	SF	SF	SF	SF	SF	SF	SF
5.10.8	Administrative processes of the loading of goods	SF	SF	SF	SF	SF	SF	SF
5.10.9	Internal control procedures	SF	SF	SF	SF	SF	SF	SF
5.11	**Security requirements for foreign suppliers business partner security**							
5.11.1	Security requirements imposed on others business partners	SF (E)	SF (E)	SF (I/E)	SF (I/E)	SF (I/E)	SF (I/E)	SF (I)
5.11.2	External control procedures	SF (E)	SF (E)	SF (I/E)	SF (I/E)	SF (I/E)	SF (I/E)	SF (I)
5.12	**Personnel security**							
5.12.1	Employment policy	SF	SF	SF	SF	SF	SF	SF
5.12.2	Security checks on prospective employees	SF	SF	SF	SF	SF	SF	SF
5.12.3	Safety and security training	SF	SF	SF	SF	SF	SF	SF
5.12.4	Safety and security requirements for temporary personnel	SF	SF	SF	SF	SF	SF	SF
5.13	**External services**							
5.13.1	External services	SF	SF	SF	SF	SF	SF	SF

1) Where appropriate
2) Only if the local clearance procedure is used
3) Where appropriate, if an economic customs procedure such as inward and/or outward processing is applied
4) Where appropriate, in particular CAP goods or where the local clearance procedure is used
(I) Import
(E) Export

I.2. Abbreviations

AEO	Authorised Economic Operator
AEO COMPACT model	Authorised Economic Operator, Compliance and Partnership Customs and Trade
Branch	Office/premise/another location of the company itself and forms part of the company's total assets and legal identity
CC	Customs Code
CCIP	Customs Code Implementing Provisions
EC	European Community
EU	European Union
ICAO	International Civil Aviation Organisation
Incoterms	Standard trade definitions and commonly used in international sales contract on who bears the costs and risks of the goods at which moment
ISO	International Standard Organisation
ISO/PAS	International Standard Organisation, Public Available Specification
ISPS Code	International Ship and Port Facility Security Code (international mandatory IMO convention)
IMO	International Maritime Organisation
OJ	Official Journal
SME	Small and Medium sized Enterprise
Subsidiaries	Multinational companies are usually consisting of a parent company and subsidiary companies, each of them being an individual legal person, i.e. an individual legal entity registered in the local company register according to the Member State's company law where the relevant subsidiary is established.
UK	United Kingdom
UNECE	United Nations Economic Commission for Europe
WCO SAFE	World Customs Organisations Safe and Secure Framework of Standards

- - - - -