



**EUROPEAN COMMISSION**

DIRECTORATE-GENERAL

TAXATION AND CUSTOMS UNION

Security, safety, Trade Facilitation, Rules of origin & International cooperation

**Risk Management and Security**

**Brussels, 11 March 2016**

**TAXUD/B2/047/2011 –Rev.6**



***AUTHORISED ECONOMIC OPERATORS***

**GUIDELINES**

Approved by the CCC-GEN (AEO subsection) on 11 March 2016

*It must be stressed that this document does not constitute a legally binding act and is of an explanatory nature.*

*Legal provisions of customs legislation take precedence over the contents of this document and should always be consulted.*

*The authentic texts of the EU legal instruments are those published in the Official Journal of the European Union.*

*There may also exist national instructions or explanatory notes in addition to this document."*

## Table of Contents

ABBREVIATIONS.....	6
PART 1, GENERAL INFORMATION .....	8
Section I - Introduction .....	9
1.I.1. AEO-Customs Simplifications (AEOC):.....	10
1.I.2. AEO-Security and Safety (AEOS):.....	11
1.I.3. AEO-Customs Simplifications/Security and Safety (AEOC/AEOS): ...	11
1.I.4. Preparation before submitting an application: .....	12
Section II - Who can become an AEO? .....	15
1.II.1. Who is an ‘economic operator’?.....	15
1.II.2. Who is an economic operator ‘established in the Union’?.....	15
1.II.3. Who is an economic operator ‘involved in customs related activities’? .....	16
1.II.4. Stakeholders in an international supply chain .....	17
Section III - AEO Benefits .....	19
1.III.1. Easier admittance to customs simplifications .....	20
1.III.2. Prior notification.....	21
1.III.3. Fewer physical and document-based controls.....	22
1.III.4. Priority treatment of consignments if selected for control .....	25
1.III.5. Choice of the place of controls.....	25
1.III.6. Indirect benefits .....	26
Section IV – Cooperation between customs and other government authorities .....	28
Section V - Mutual recognition.....	29
Section VI – The AEO Logo.....	30
PART 2, AEO CRITERIA .....	31
Section I - Compliance with customs legislation and taxation rules, including no records of serious criminal offences relating to the economic activity of the applicant .....	31
2.I.1. General.....	31
2.I.2. Infringements of minor importance .....	32
2.I.3. Repeated infringements.....	33
2.I.4. Serious infringements .....	34
Section II - Satisfactory system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls.....	35
2.II.1. General.....	35
2.II.2 Condition of satisfactory system of managing commercial and transport records .....	36
Section III - Proven financial solvency .....	40

2.III.1. General .....	40
2.III.2. Sources of information .....	41
2.III.3. Finance from a loan from another person or a financial institution ....	44
2.III.4. Letters of comfort and guarantees from parent (or other group) companies .....	45
2.III.5. Applicants established in the EU for less than three years.....	45
Section IV - Practical standards of competence or professional qualifications directly related to the activity carried out.....	46
2.IV.1. General .....	46
2.IV.2. Practical Standards .....	47
2.IV.3. Professional qualifications .....	51
Section V - Appropriate security and safety standards .....	52
2.V.1. General .....	52
2.V.2. Building security .....	54
2.V.3. Appropriate access controls.....	55
2.V.4. Cargo security.....	56
2.V.5. Business Partner Security .....	57
2.V.6. Personnel security.....	60
2.V.7. External service providers .....	62
2.V.8. Security awareness programmes .....	63
2.V.9. Appointed contact person .....	64
<b>PART 3, APPLICATION AND AUTHORISATION PROCESS.....</b>	<b>65</b>
Section I - Determination of the competent Member State for submitting an AEO application .....	66
3.I.1. General: .....	66
3.I.2. Accessibility of customs related documentation.....	66
3.I.3. Multinational companies and large businesses .....	67
Section II - Receipt and acceptance of the application .....	69
Section III - Risk analysis and Auditing process .....	70
3.III.1. Collect and analyse information.....	70
3.III.2. Small and medium-sized enterprises.....	71
3.III.3. Specific economic activities.....	72
3.III.4. Factors facilitating the authorisation process .....	77
3.III.5. Parent/subsidiary companies with common system/procedures .....	83
3.III.6. Risk and risk analysis .....	84
3.III.7. Auditing and risk based audit.....	87
Section IV - Decision about granting of the status.....	90
3.IV.1. Factors to be considered before taking the decision .....	90
3.IV.2. Taking the decision .....	91
3.IV.3. Informing the applicant .....	91
3.IV.4. Appeals.....	92
3.IV.5. Time-limits.....	93

PART 4, EXCHANGE OF INFORMATION BETWEEN MEMBER STATES AND WITH OTHER GOVERNMENT AUTHORITIES.....	94
Section 1 - Exchange of information between Member States .....	94
4.I.1. Information procedure.....	94
4.I.2. Consultation procedure .....	95
4.I.3. Means of communication.....	96
Section II – Exchange of information between customs and other government authorities .....	97
PART 5, MANAGEMENT OF THE AUTHORISATION .....	99
Section I - Monitoring .....	99
5.I.1. General.....	99
5.I.2. AEO authorisation covering several PBEs .....	103
Section II – Re-assessment.....	104
5.II.1. Re-assessment following changes to the EU legislation .....	104
5.II.2. Re-assessment following the result of a monitoring carried out or due to information provided by the holder of the decision or by other authorities .....	104
Section III – Amendment of the decision.....	105
Section IV - Suspension .....	106
Section V - Revocation .....	108
PART 6, MUTUAL RECOGNITION .....	109
Section I - Mutual Recognition Agreements concluded by the EU .....	109
Section II - Process steps towards Mutual Recognition.....	109
Section III - Implementation and follow-up after the signature of an MRA.....	109
Section IV - MRA Benefits proposed by the EU for members of partner AEO programmes (and reciprocal).....	110
Section V - Implementation of MRAs – How to benefit from MRAs? .....	111
Section VI - Unilateral Suspension of Benefits .....	111
Section VII - Recommendations for conducting an AEO audit or monitoring visit in an EU Member State .....	112
PART 7, ANNEXES .....	114

## Abbreviations

<b>AEO</b>	Authorised Economic Operator
<b>AEOC</b>	AEO – Customs Simplifications
<b>AEOs</b>	AEO - Security and Safety
<b>AC</b>	Account Consignor
<b>CCC</b>	Community Customs Code <sup>1</sup>
<b>CCIP</b>	Customs Code Implementing Provisions <sup>2</sup>
<b>EC</b>	European Community
<b>EORI</b>	Economic Operator Registration and Identification
<b>EOS</b>	Economic Operator System
<b>ERP</b>	Enterprise resource planning
<b>EU</b>	European Union
<b>ICA</b>	Issuing Customs Authority
<b>ICAO</b>	International Civil Aviation Organisation
<b>ISO</b>	International Standard Organisation
<b>ISO/PAS</b>	International Standard Organisation, Public Available Specification
<b>IMO</b>	International Maritime Organisation
<b>KC</b>	Known Consignor
<b>LSE</b>	Large Scale Enterprise
<b>MRA</b>	Mutual Recognition Agreement
<b>MS</b>	Member State(s) of the EU
<b>OJ</b>	Official Journal
<b>OTIF</b>	Intergovernmental Organisation for International Carriage by Rail
<b>PBE</b>	Permanent Business Establishment
<b>RA</b>	Regulated Agent
<b>RBA</b>	Risk-based audit
<b>SME</b>	Small and Medium sized Enterprise
<b>SAQ</b>	Self-assessment questionnaire
<b>TAPA</b>	Transported Asset Protection Association
<b>TAXUD</b>	General Directorate 'Taxation and Customs Union'
<b>UNECE</b>	United Nations Economic Commission for Europe
<b>UPU</b>	Universal Postal Union
<b>UCC</b>	Union Customs Code <sup>3</sup>
<b>UCC DA</b>	Union Customs Code Delegated Act <sup>4</sup>
<b>UCC IA</b>	Union Customs Code Implementing Act <sup>5</sup>

---

<sup>1</sup> Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code

<sup>2</sup> Commission Regulation (EEC) No 2454/93 of 2 July 1993 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code

<sup>3</sup> Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code

<sup>4</sup> Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council with regard to detailed rules of specifying some of the provisions of the Union Customs Code

**WCO**  
**WCO SAFE**

World Customs Organisation  
World Customs Organisations Safe Framework of  
Standards to Secure and Facilitate Global Trade

---

<sup>5</sup> Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code

## **PART 1, General information**

The AEO concept is based on the Customs-to-Business partnership introduced by the World Customs Organisation (WCO). Traders who voluntarily meet a wide range of criteria work in close cooperation with customs authorities to assure the common objective of supply chain security.

The concept is strongly based on the partnership of customs with the economic operator. This implies that the relationship between customs and AEO should be always based on the principles of mutual transparency, correctness, fairness and responsibility. Customs expects the AEO to act in line with customs legislation and to inform customs about any difficulties to comply with the legislation. Customs should provide support to achieve this.

The EU established its AEO concept based on the internationally recognised standards, creating a legal basis for it in 2008 through the 'security amendments' to the "Community Customs Code" (CCC) and its implementing provisions. The programme, which aims to enhance international supply chain security and to facilitate legitimate trade, is open to all supply chain actors. It covers economic operators authorised for customs simplification (AEOC), security and safety (AEOS) or a combination of the two.

These Guidelines do not constitute a legally binding act and are of an explanatory nature. Their purpose is to ensure a common understanding for both customs authorities and economic operators and to provide a tool to facilitate the correct and harmonised application by Member States of the legal provisions on AEO. They constitute a single document together with its annexes covering all main tools used during the AEO application and management procedure. These Guidelines are updated on a regular basis to reflect legal developments and to include practical experience gained so far as well as best practices acquired.

The latest version of the AEO Guidelines is published on the website of DG TAXUD:

[http://ec.europa.eu/taxation\\_customs/customs/policy\\_issues/customs\\_security/aeo/index\\_en.htm](http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm).

### **How to use these Guidelines?**

[Part 1](#) of the Guidelines provides general information about the EU AEO programme including the benefits of the status and mutual recognition.

[Part 2](#) of the Guidelines describes the AEO criteria and the different aspects of the security requirements and supply chain security.

[Part 3](#) of the Guidelines deals with the overall decision-making process concerning both customs authorities and economic operators.

[Part 4](#) of the Guidelines describes different aspects of the exchange of information between customs authorities including consultation.

[Part 5](#) of the Guidelines covers all aspects related to the management of the already granted status, including monitoring, re-assessment, amendment, suspension and revocation.

[Part 6](#) of the Guidelines deals with Mutual Recognition of AEO Programmes

[Part 7](#) of the Guidelines contains the Annexes.

[Annex 1](#) includes the Self-assessment questionnaire (SAQ) and its Explanatory Notes. According to Article 26 Union Customs Code Delegated Act (UCC DA) in order to apply for



the status of AEO the applicant shall submit a self-assessment questionnaire, which the customs authorities shall make available, together with the application.

[Annex 2](#) includes the document 'Threats, Risks and Possible solutions' which is addressed both to customs authorities and economic operators. It aims at facilitating the audit and the examination to ensure compliance with AEO criteria by matching the information provided in the SAQ and the risk areas identified and also provide examples of possible solutions to cover the risks and threats identified.

[Annex 3](#) includes an example of a template for security declaration.

[Annex 4](#) includes a list of examples of information to be shared with customs authorities according to Article 23 (2) Union Customs Code (UCC).

## **Section I - Introduction**

### **The AEO status**

An AEO can be defined as an economic operator as laid down in Article 5 (5) UCC who is deemed reliable in the context of his or her customs related operations, and therefore, is entitled to enjoy benefits throughout the EU.

The AEO programme is open to all economic operators, including small and medium sized enterprises ([see Part 3, Section III.2 'Small and Medium sized enterprises' of these Guidelines](#)) and regardless of their role in the international supply chain.

There is no legal obligation for economic operators to become an AEO, it is a matter of the operators own choice based on their specific situation. Nor is there any legal obligation for AEOs to require their business partners to obtain the AEO status.

According to Article 38 UCC the status of the authorised economic operator consists of different types of authorisations: AEO for Customs Simplification (AEOC) and AEO for Security and Safety (AEOS). Each type of authorisation offers different types of benefits.

On the basis of Article 39 UCC, the AEO status can be granted to any economic operator meeting the following common criteria:

- record of compliance with customs legislation and taxation rules, including no record of serious criminal offences relating to the economic activity of the applicant,
- demonstration of a high level of control of its operations and of the flow of the goods, by means of a system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls,
- proven financial solvency.

And depending on the type of AEO status

- practical standards of competence or professional qualifications directly related to the activity carried out (AEOC),
- appropriate security and safety standards (AEOS).

The AEO status granted by one Member State is recognised by the customs authorities in all Member States (Article 38 (4) UCC).

### **1.I.1. AEO-Customs Simplifications (AEOC):**

An AEO status in the form of an AEOC is envisaged for economic operators established in the Union who would like to benefit from the various simplifications specifically provided for under the customs legislation.

The criteria for granting of an AEOC include:

- the absence of any serious infringement or repeated infringements of customs legislation and taxation rules, including no record of serious criminal offences relating to the economic activity of the applicant;
- demonstration by the applicant of a high level of control of his or her operations and of the flow of goods, by means of a system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls;
- financial solvency, which shall be deemed to be proven where the applicant has good financial standing, which enables him or her to fulfil his or her commitments, with due regard to the characteristics of the type of business activity concerned; practical standards of competence or professional qualifications directly related to the activity carried out.

As these criteria apply to most customs simplifications/authorisations, obtaining an AEOC would facilitate the economic operator's eligibility and usage of the various simplifications/authorisations. For example in line with Article 211 (3) (b) UCC, the criteria for the authorisations for special procedures are taken into account during the AEO application process. Further, for other simplifications or authorisations the AEOC status is required to have access to some simplifications/authorisations such as the entry into declarant's record with a waiver of the obligation for the goods to be presented as provided for Article 182 UCC.

An AEOC is entitled to:

- benefit from specific types of simplifications on the basis of the recognition of the AEOC as long as the requirements related to a specific type of simplification provided for in the customs legislation are fulfilled;
- more favourable treatment than other economic operators in respect of customs controls, including fewer physical and document-based controls, with the exception of controls related to security and safety measures;
- prior notification in case of selection for customs control;
- priority treatment if selected for control;
- possibility to request a specific place for such control.

See also Part 1, Section III 'AEO Benefits'.

The criterion for appropriate security and safety standards is not required for this type of AEO authorisation. Therefore holders of AEOC are not entitled to any of the AEO benefits related to security and safety of the international supply chain. The AEO status in the form of AEOC is currently not taken into account with respect to Mutual Recognition Agreements (MRA) with third countries.

### **1.I.2. AEO-Security and Safety (AEOS):**

An AEOS is envisaged for economic operators established in the Union who would like to benefit from particular facilitations related to customs controls relating to security and safety when the goods enter or leave the customs territory of the Union.

The criteria for granting of AEOS include:

- a record of compliance with customs legislation and taxation rules, including no record of serious criminal offences relating to the economic activity of the applicant;
- demonstration of a high level of control of its operations and of the flow of the goods, by means of a system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls. However, unlike an AEOC, an AEOS is not required to have a logistical system which distinguishes between Union and non-Union goods within their records;
- proven financial solvency; and
- appropriate security and safety standards.

An AEOS is entitled to:

- facilitations regarding pre-departure declarations;
- more favourable treatment than other economic operators in respect of customs controls, including fewer physical and document-based controls in respect of security and safety;
- prior notification in case of selection for customs control;
- priority treatment if selected for control;
- possibility to request a specific place for such control.

An AEOS is recognised as an economic operator who has taken appropriate measures to secure his or her business and is thus a reliable actor in the international supply chain both from the perspective of the relevant government authorities and from the perspective of his or her business partners. The AEOS is taken into account with respect to MRAs with third countries.

See also Part 1, Section III 'AEO Benefits'.

### **1.I.3. AEO-Customs Simplifications/Security and Safety (AEOC/AEOS):**

Both types of authorisations, AEOC and AEOS, may be held at the same time. In this case, the operator has to fulfil the criteria for AEOC and AEOS and receives the benefits relating to both.

Article 33 UCC Implementing Act (UCC IA) lays down that *"where an applicant is entitled to be granted both an AEOC and an AEOS authorisation, the customs authority competent to take the decision shall issue one combined authorisation"*.

For the purpose of the management of the AEOC and AEOS authorisation held at the same time by an economic operator, the electronic exchange of information pursuant to Article 16 (1) UCC takes place via a unique AEO authorisation number (which currently has the structure of country code followed by letters AEOF and the national authorisation number).

The following table summarises the AEO conditions and criteria:

Conditions and criteria	AEOC	AEOS	Reference UCC/UCC IA	Guidelines Part
Economic Operator	X	X	Art. 5 (5) UCC	1.II.1
Established in the Customs Territory of the Union	X	X	Art. 5 (31) UCC	1.II.2
Compliance	X	X	Art. 39 a) UCC Art. 24 UCC IA	2.I
Appropriate Record Keeping	X	X	Art. 39 b) UCC Art. 25 UCC IA	2.II
Financial Solvency	X	X	Art. 39 c) UCC Art. 26 UCC IA	2.III
Practical Standards of Competence and Professional Qualification	X		Art. 39 d) UCC Art. 27 UCC IA	2.IV
Security & Safety		X	Art. 39 e) UCC Art. 28 UCC IA	2.V

#### **1.I.4. Preparation before submitting an application:**

The preparation of the AEO application, as well as the authorisation and the maintenance of the AEO, is a time consuming process. Thorough preparation is the key to success. Therefore it is expected, that the applicant who wants to become an AEO is in control of his or her business.

This means that depending on the type of AEO applied for and the company's business activities and business model, the company should have in place appropriate organisational measures in the fields related to the AEO criteria, aiming at ensuring that risks linked to his or her customs activities may be identified and avoided and/or minimised.

To better understand what customs mean by this and to speed up the process, the usage of a [SAQ](#) is compulsory.

The [SAQ](#) is a tool to structure the preparation of the economic operator, to identify the organisational units within the operator to be included and to understand the necessary depth of preparation.

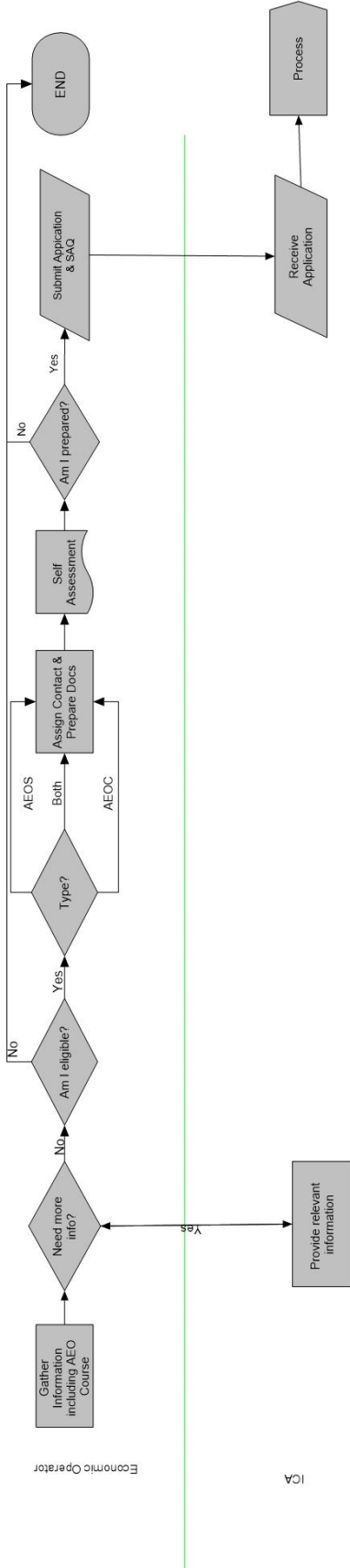
For a close cooperation between customs and the applicant/AEO it is recommended to get in contact with the Issuing Customs Authority (ICA) at an early stage and to keep that contact even beyond the application process. This can help to avoid misunderstandings on both sides and gives support if any questions arise.

In summary, before formal submission of the application, the economic operator is strongly recommended to:

- contact the ICA,
- decide on the type of authorisation required,
- nominate a competent contact person in charge of the application,
- fill out thoroughly the [SAQ](#) and ensure that all the relevant persons/departments within the organisation are involved in the filling of the [SAQ](#).

In addition, it is necessary to ensure that the management of the company supports the AEO application.

The following flowchart provides an overview of the preparation process:



[See also Part 3 on Application and authorisation process.](#)

## **Section II - Who can become an AEO?**

Article 38 (1) UCC stipulates that an economic operator who is established in the customs territory of the Union and who meets the criteria set out in Article 39 UCC may apply for the status of AEO.

This basic requirement implies fulfilment of two conditions: the applicant being an economic operator **and** being established in the customs territory of the Union.

### **1.II.1. Who is an ‘economic operator’?**

Article 5 (5) UCC provides that *“Economic operator means: a person who, in the course of his or her business, is involved in activities covered by the customs legislation”*.

Again the legal definition of ‘economic operator’ implies two main conditions. The applicant has to be a ‘person’ and has to be involved in activities covered by customs legislation.

Pursuant to Article 5 (4) UCC “person” means:

- a natural person,
- a legal person,
- and any association of persons which is not a legal person, but which is recognised under Union or national law as having the capacity to perform legal acts.

However, the national law of each Member State defines who is considered a natural person, a legal person or an association of persons recognised as having the capacity to perform legal acts but lacking the legal status of a legal person.

Multinational companies usually consist of a parent company and subsidiary companies or/and branches.

A subsidiary is an individual legal person, i.e. an individual legal person or an association of persons 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, the applications must be submitted by all the subsidiary companies wishing to become an AEO.

A "branch", on the other hand, is an office/premise/another location of the company itself and forms part of the company's total assets and thus is not an individual legal person. In this case a single application, covering all the EU branches that are not individual legal persons or association of persons, has to be submitted by the parent company wishing to acquire the AEO status. In order to identify the competent Member State where to submit the single application see Part 3, Section I ‘Determination of the competent Member State for submitting an AEO application’.

### **1.II.2. Who is an economic operator ‘established in the Union’?**

Pursuant to Article 5 (31) UCC, a person is established in the customs territory of the Union, if:

- in the case of a natural person, any person who has his or her habitual residence in the customs territory of the Union,;

- in the case of a legal person or an association of persons, any person having its registered office, central headquarters or a permanent business establishment (PBE) in the customs territory of the Union.

Article 5 (32) UCC defines "permanent business establishment" as *a fixed place of business where both the necessary human and technical resources are permanently present and through which a person's customs-related operations are wholly or partly carried out.*

Multinational or big companies usually consist of a parent company and subsidiaries or branches which can be established in one or several Member States. Although being a PBE of the same parent company these companies can have different legal status in the different Member States as the legal form under which they operate in Member States depends on how they have chosen to operate and mainly on the national legislation of the Member State concerned. As a result a parent company may have some of its branches considered as individual legal persons in some Member States (i.e. an individual legal person registered in the local company register according to the Member State's company law) and also some PBEs are not considered as being individual legal person in other Member States.

In this case an economic operator which wants to apply for an AEO status for all its PBEs has to assess in which group they belong. In case they are legal persons or fall under the definition of persons described in Article 5(4) UCC, they have to apply separately for an AEO status in the relevant Member State. In all other cases they cannot apply separately for an AEO status; instead a single application covering all of them shall be submitted by the parent company considered a person in accordance with the EU legislation.

Customs authorities should also consider that the general conditions are the same for all kinds of authorisations/decisions for which the economic operator applies for. For example customs cannot deem an economic operator to be a legal person when applying for example for an EORI number and deem it to be a simple branch when it applies for AEO status while using the same legislation to do so.

### **1.II.3. Who is an economic operator ‘involved in customs related activities’?**

The other aspect that has to be considered when establishing whether a particular applicant is an ‘economic operator’ is whether his or her economic activity is ‘covered by customs legislation’.

Applications for AEO status may only be accepted from an economic operator who in the course of his or her business is involved in activities covered by the customs legislation. On the basis of this definition there are a number of situations where the economic operator cannot apply for an AEO status as he or she is not involved in customs activities, e.g.:

- an EU based supplier who distributes only goods already in free circulation to an EU based manufacturer;
- a transport operator that moves only goods in free circulation which are not under any other customs procedure within the customs territory of the Union;
- a manufacturer producing goods only for the EU internal market and using raw materials already in free circulation;
- a consultant who is only consulting/providing opinion in customs matters.



The definition of economic operator does not restrict the notion of "involvement in activities covered by the 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 customs related data regarding these goods can apply for AEOS.

However, each case has to be treated separately with due account of all the circumstances relevant for the particular economic operator.

#### **1.II.4. Stakeholders in an international supply chain**

The international end-to-end supply chain from a customs perspective represents the process, e.g. from manufacturing goods destined for export until delivery of the goods to the buyer in another customs territory (being the customs territory of the Union or another customs territory). The international supply chain is not a discrete identifiable entity. It is a series of ad hoc constructs comprised of economic operators representing various trade industry segments. In some cases the economic operators are all known and a long-term relationship may exist, whilst in other cases economic operators may change frequently or may only be contractually related for a single operation/shipment. From an operational point of view the reference to "supply chains" instead of "supply chain" is better, meaning that any economic operator may be involved not just in one theoretical supply chain but in many practical ones.

In practice, many businesses can have more than one role in a particular supply chain and will fulfil more than one of the responsibilities related to these roles (e.g. a freight forwarder can also act as a customs representative). When applying for AEO status the applicant must ensure his or her application includes the customs related activities for all their responsibilities within the international supply chain.

The various stakeholders and their different responsibilities in the international supply chain, relevant from a customs perspective which can apply for an AEO status are mainly the following:

##### **a) manufacturer**

In the framework of the international supply chain a manufacturer is an economic operator who in the course of his or her business produces goods destined for export.

A manufacturer's responsibility in the international supply chain can be, *inter alia*:

- ensure a safe and secure manufacturing process for its products;
- ensure a safe and secure supply of its products to its clients;
- ensure the correct application of customs rules with regard to the origin of the goods.

##### **b) exporter**

For the purpose of AEO an exporter, pursuant to Article 1 (19) UCC DA means:

- the person established in the customs territory of the Union who, at the time when the declaration is accepted, holds the contract with the consignee in the third country and has the power for determining that the goods are to be brought to a destination outside the customs territory of the Union,

- in other cases, the person established in the customs territory of the Union who has the power for determining that the goods are to be brought to a destination outside the customs territory of the Union.

An exporter's responsibility in the international supply chain can be, *inter alia*:

- responsible for the correctness of the export declaration and for its timely lodgement, if the export declaration is lodged by the exporter;
- responsible for lodging an export declaration with the prescribed data requirements;
- apply the legal export formalities in accordance with the customs rules, including commercial policy and prohibition and restriction measures and where appropriate, export duties;
- ensure a secure and safe supply of the goods to the carrier or freight forwarder or customs agent.

### **c) 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 acts as a carrier and issues its own transport contract, e.g. bill of lading. 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, *inter alia*:

- apply the rules on transport formalities
- ensure, if relevant, a secure and safe transport of goods
- apply, where appropriate, the rules on summary declarations in accordance with the legislation

### **d) warehouse keepers and other storage facility operators**

A warehouse-keeper is a person authorised to operate a customs warehouse or a person operating a temporary storage facility, or free zone facilities.

A warehouse-keeper's responsibility in the international supply chain can be, *inter alia*:

- ensure that while the goods are in a customs warehouse or in a temporary storage, adequate procedures are in place ensuring that they are not removed from customs supervision and fulfil other 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 authorisation for the customs warehouse or for the temporary storage facility;
- provide an adequate protection of the storage area against external intrusion;
- provide an adequate protection against unauthorised access to, substitution of and tampering with the goods.

### **e) customs agent/representative**

A customs agent, as referred to in these Guidelines is a person who performs customs formalities acting as a customs representative as laid down in Article 18 UCC. A customs representative acts 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 or her own name (indirect representation).

A customs agent's responsibility in the international supply chain can be, *inter alia*:

- to apply the necessary provisions in accordance with the customs rules specific for the type of representation, for placing the goods under a customs procedure;

- responsible for the correctness of the customs or summary declaration and for its timely lodgement.

#### **f) carrier**

In general, a carrier is the person actually transporting the goods or who has undertaken a contract, and issued e.g. a bill of lading or air waybill, for the actual carriage of the goods. A concrete definition of the carrier is included in Article 5 (40) UCC.

The carrier's responsibility in the international supply chain can be, *inter alia*:

- ensure a secure and safe transport of goods while in the carrier's custody, in particular avoiding unauthorised access to and tampering with the means of transport and the goods being transported;
- provide timely transport documentation as required by law;
- apply the necessary legal formalities in accordance with customs law;
- apply, where appropriate, the rules on summary declarations in accordance with the legislation.

#### **g) importer**

An importer is an economic operator who is making or on whose behalf an import declaration is made. However, from a more general trade perspective and in particular with a view to the substance of the AEO programme, the definition of the real importer should be considered from a more broader perspective (the person making the import declaration is not necessarily always the person who also places the goods on the market).

An importer's responsibility in the international supply chain can be, *inter alia*:

- responsible in his or her dealings with the customs authorities, for assigning the goods presented to customs a customs-approved treatment or use;
- responsible for the correctness of the declaration and that it will be lodged in time;
- where the importer is the person lodging the entry summary declaration 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;
- apply commercial policy and prohibition and restriction measures;
- ensure a secure and safe receipt of goods, in particular avoiding unauthorised access to and tampering with the goods.

**h) others**, for example, terminal operators, stevedores and cargo packers.

### **Section III - AEO Benefits**

The AEO authorisation is issued to the applicant, after a thorough audit of his or her business activity, and not to his or her business partners. The AEO status granted relates to the economic operator itself and applies to its own business activities and he is the only one entitled to receive the benefits. This is a general principle for all types of AEO that can be issued to economic operators with different roles in the international supply chain.

The AEO status shall be recognised across all Member States, pursuant to Article 38 (4) UCC therefore, the holder of an AEO authorisation shall receive the same benefits in all Member States.

AEO benefits are an integral part of the EU legislation governing the AEO status.

The AEO benefits, dependant on the type of the authorisation, are summarised below.

To enable customs authorities to deliver these benefits, the AEO should ensure its EORI number is declared to customs.

### **1.III.1. Easier admittance to customs simplifications**

This benefit is applicable to holders of an AEOC authorisation.

The EU customs legislation provides for the following cases where the AEO takes value:

- a) the AEO status is required to have access to a simplification/authorisation,
- b) some of the criteria for a particular simplification/authorisation are covered by AEO criteria,
- c) the criteria for a particular simplification/authorisation are considered equivalent to AEO criteria .

Article 38 (5) UCC provides that if the person requesting a particular simplification is the holder of an AEOC authorisation, customs authorities shall not re-examine those conditions which have already been examined when granting the AEO status. This means that customs authorities should focus on new or additional elements and requirements relating to the respective simplification.

The criteria which are deemed to be met by an AEO can be found in the appropriate Articles of the UCC and its implementing provisions related to the specific simplification. A list of the simplifications concerned is provided below.

- a) Cases where the AEO status is required to have access to a simplification/authorisation:
  - Comprehensive guarantee with reduced amount for existing customs debts and charges, Article 95 (3) UCC,
  - Centralised clearance (where an authorisation is required), Article 179 (2) UCC,
  - Entry into declarant's records with a waiver of the obligation for the goods to be presented, Article 182 (3) UCC,
  - Self-assessment, Article 185 UCC and Article 151 UCC DA.
  
- b) Cases where some of the criteria for a particular simplification/authorisation are covered by AEO criteria (application of Article 38 (5) UCC):
  - Customs representative providing services in a Member State other than the one where he or she is established, Article 18 (3) UCC,
  - Authorisation for simplification related to value of goods for customs purposes, Article 71 UCC DA,
  - Comprehensive guarantee, Article 95 (1) UCC,
  - Comprehensive guarantee or a waiver guarantee in respect of customs debts and other charges which may be incurred, Article 95 (2) UCC,
  - Authorisation to use a temporarily prohibited comprehensive guarantee, Article 96 (2) UCC,
  - Approval of a place other than the competent customs office (presentation of the goods), Article 115 UCC DA,
  - Authorisation for a regular shipping service, Article 120 UCC DA,

- Authorised issuer (proof of customs status), Article 128 UCC DA,
- Authorised banana weigher, Article 155 UCC DA,
- Authorisation for simplified customs declaration, Article 145 UCC DA,
- Authorisation for entry in declarant's records, Article 150 UCC DA,
- Authorised consignee (TIR), Article 187 UCC DA,
- Authorisation for simplifications related to transit, Article 191 UCC DA.

c) Cases where the criteria for a particular simplification/authorisation are considered equivalent to AEO criteria:

- Authorisation for the operation of temporary storage facility, Article 148 (2) (b) and (4) 3<sup>rd</sup> subparagraph UCC,
- Authorisation for special procedures, Articles 211 (3) (b), 214 (2) and 223 (2) 2<sup>nd</sup> subparagraph UCC.

It is to be noted that the AEO status was introduced in the EU customs legislation after the other simplifications and therefore the majority of economic operators have already been authorised for them before they get the AEO status. Nevertheless, this particular benefit is still very important for AEOs, or those considering applying for an AEO status, and even more for customs authorities. In terms of planning any monitoring activities for the AEO they would be coordinated with those for other authorisations granted and thus avoiding duplication as much as possible. In order that this benefit is used in the most efficient way both for AEOs and for customs authorities, the following should be taken into account:

- as simplifications are conditional on compliance with certain AEO criteria, the relationship/dependency between the specific authorisation and the AEO status have to be ensured/kept throughout the process, covering not only the application phase but also the monitoring and re-assessment once the authorisation/status are granted;
- the examination of the relevant AEO criteria before granting the status of an AEO is not an 'abstract' exercise and is always done against the particular business activities that the economic operator has. Therefore, when an application for a specific authorisation is submitted customs authorities should not re-examine the criteria which have been already checked but focus only on any new elements/requirements.

For further details please see also "Simplifications – Title V UCC/ "Guidance for MSs and Trade" (TAXUD/A2/31/03/2016).

[http://ec.europa.eu/taxation\\_customs/sites/taxation/files/resources/documents/customs/customs\\_code/guidance\\_simplifications\\_en.pdf](http://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/customs_code/guidance_simplifications_en.pdf)

### **1.III.2. Prior notification**

This benefit that provides the AEO authorisation holder with a logistic advantage by being able to better plan and optimise transport and logistics more sufficiently, minimise logistic delay and reduce transport costs can apply:

a) to holders of both AEOC and AEOs:

Article 38 (6) UCC and Article 24 (3) UCC DA foresee that *"where an AEO lodges a temporary storage declaration or a customs declaration in accordance with Article 171 of the Code, the customs office competent to receive that temporary storage declaration or that customs declaration shall, where the consignment has been selected for customs control,*

*notify the AEO of that fact. That notification shall take place before the presentation of the goods to customs.*

*That notification shall not be provided where it may jeopardise the controls to be carried out or the results thereof."* This also includes controls on behalf of other governmental authorities, where applicable.

It is important that the distinction between prior notifications related to security and safety and prior notifications related to application of other measures provided for in the customs legislation is made.

This means that only AEOS shall receive prior notification in case of security and safety related customs controls whereas AEOC shall receive prior notification in case of not security related customs controls.

b) to holders of AEOS only:

Article 24 (2) UCC DA lays down that when an entry summary declaration has been lodged by an AEO, the customs office of first entry shall notify the AEO in case the consignment has been selected for physical control. That notification shall take place before the arrival of the goods in the customs territory of the Union provided the AEO is connected to the electronic customs systems. The prior notification might be particularly important for AEO operating at big ports as it will allow them better planning of their business.

That notification shall not be provided where it may jeopardise the controls to be carried out or the results thereof. The customs authorities may, however, carry out physical control even where the AEO has not been notified.

### **1.III.3. Fewer physical and document-based controls**

This benefit is applicable to holders of both AEOC and AEOS.

Article 38 (6) UCC and Article 24 (1) UCC DA lay down that an AEO shall be subject to fewer physical and document-based controls than other economic operators in respect of customs controls, according to the type of authorisation granted. However, the customs authorities may decide to control shipments of an AEO in order to take into account a specific threat, or control obligations set out in other Union legislation (i.e. related to product safety etc.).

At the same time there are also examples where the AEO status is favourably taken into account even for other controls<sup>6</sup>.

It is also important that the distinction between controls related to security and safety and controls related to application of other measures provided for in the customs legislation is made.

---

<sup>6</sup> **Commission regulation (EC) No 1276/2008 of 17 December 2008 on the monitoring by physical checks of exports of agricultural products receiving refunds or other amounts**

This means that only AEOS shall benefit from fewer physical and document-based controls related to security and safety whereas AEOC shall benefit from fewer physical and document-based controls related to other measures provided for in the customs legislation. This includes fewer controls at the point of importation or exportation and can be taken into account for post clearance controls as well.

To deliver this benefit, a lower risk score should be incorporated into the customs risk management systems. Nevertheless, while the lower risk score is due to the fact that the status of the AEO is always favourably taken into account, the level of reduction can vary depending on the role and responsibility of the AEO in the particular supply chain.

It has to be also taken into account that this benefit is related with the overall risk assessment done for a particular transaction. Thus, although the AEO status would always count for favourable treatment other risk indicators e.g. country of origin etc. might trigger the necessity for a control to be done.

Taking the abovementioned general principles into consideration the following are some examples of potential situations:

*a) entry summary declaration (ENS):*

In most of the cases the requirements and responsibilities for submitting an ENS are for the carrier. In case he is the person submitting the ENS and is a holder of an AEOS, he is directly entitled to receive lower risk scores being his or her systems and procedures related to security of conveyance, business partners, employees already examined by customs authorities. If in addition to the carrier also the consignee is holder an AEOS the level of controls could be further reduced.

Besides, if the declared consignor also holds an equivalent AEO authorisation issued by a customs authority in a third country which is recognised by the EU under a mutual recognition agreement (see [Part 1, Section V](#) and [Part 6 of these Guidelines](#) on 'Mutual recognition') all parties declared in the ENS, including those who have direct information of the goods involved, would have had their security and safety systems verified by customs authorities, either in the EU or by a comparable process by customs authorities in the third country. This would contribute to maximise the security of the end to end supply chain and result in an even higher level of reduction of controls related to security and safety.

There might be also cases where the data necessary for ENS are submitted through a customs declaration (e.g. for transit). The level of reductions is assessed in the same way by taking into consideration what is the role and responsibilities of the actors involved. For example, a freight forwarder who is a holder of an AEO status is the principal in a customs declaration for transit with the data set for ENS. In this case, the type of the authorisation should be considered first. In case the freight forwarder is a holder of an AEOC, the risk scores related to the customs procedure concerned can be reduced accordingly as for the traditional customs declaration for transit, the freight forwarder is the principal. He bears (even financial) responsibility for the goods carried and for the accuracy of the information given as well as for the compliance with the transit rules from the office of departure till the office of destination.

However, for reductions of risk scores related to security and safety controls the principal shall be holder of AEOS.

It is to be noted that new ENS data requirements and filing arrangements will involve different actors in the supply chain whose AEO status would need to be taken into consideration. However, this new regime will be applied only once the new ICS 2.0 will be operational.

*b) customs declaration with security and safety data for exit summary declaration (EXS) included:*

In most of the cases the exporter provides the security and safety data through the export customs declaration. Therefore, in general, if the exporter is a holder of an AEOS he or she gets higher level of reductions in terms of security and safety controls.

*c) customs declarations (security and safety data for ENS/EXS not included):*

- the holder of an AEOC is a customs agent and the client he or she is representing is a non-AEO. The AEO customs agent is lodging a customs declaration for free circulation:

In general, the customs authorities should lower the risk score in accordance with the degree of the AEO customs agent's involvement into the representation of his or her client. This is depending on the type of representation.

Allocation of benefits is related to the notion of 'Declarant'. It is important to note that according to Article 5 (15) UCC the 'Declarant' means "*the person lodging a customs declaration, a temporary storage declaration, an entry summary declaration, a re-export declaration or a re-export notification in his or her own name or the person in whose name such a declaration or notification is lodged*".

In case of direct representation, the customs agent is a direct representative of the importer which means that the customs agent acts in the name of the importer. Thus "the AEO holder" (the customs agent) and "the declarant" (the importer) are not the same persons.

Taking into consideration that customs authorities have checked the customs routines and procedures of the customs agent, his or her AEO status should be positively taken into account. However, at the same time it should be also taken into account that in this case the one responsible for the accuracy of the information given in the customs declaration, authenticity of the documents presented and compliance with all the obligations relating to the entry of the goods in question under the procedure concerned is the declarant (the importer who is not an AEO) and not the AEO holder.

In case of indirect representation, the customs agent who is the holder of the AEO status is acting in his or her own name. He or she is the 'declarant' and his or her procedures in place for bearing the responsibilities enshrined in Article 5 (15) UCC have been verified by customs authorities.

- the holder of an AEOC is an importer and he or she works with a customs agent who is not an AEO. The importer is lodging a customs declaration for free circulation:

The management of the risk should also be treated in accordance with the degree of involvement of the customs agent into his or her client's dealings with customs authorities.



#### **1.III.4. Priority treatment of consignments if selected for control**

This benefit is applicable to holders of both AEOC and AEOS.

Article 24 (4) first subparagraph UCC DA lays down that where consignments declared by an AEO have been selected for physical or document-based control, those controls shall be carried out as a matter of priority.

The granting of this benefit is directly related, and dependent upon, the mode of transport involved and the infrastructure of the facility where the controls take place.

#### **1.III.5. Choice of the place of controls**

This benefit is applicable to holders of both AEOC and AEOS.

Article 24 (4) second subparagraph UCC DA provides the possibility that on request from an AEO the controls may be carried out at a place other than the place where the goods have to be presented to customs. This alternative location might offer a shorter delay and/or lower costs. However, this is subject to individual agreements with the customs authority concerned. The selected place for control should always allow customs authorities to carry out the necessary controls and not jeopardise the results of the controls.

Although the possibility for choice of the place of controls is also provided under Article 238 second subparagraph UCC IA for all economic operators under other conditions and procedures, there is a distinction between the general provisions and the provision in the form of a benefit for AEOs, as customs can take account of the status in determining whether to grant the request.

Several practical situations may appear in terms of AEO, for example:

*- on a case by case base, for particular transactions an AEO can ask for another place where the controls are to be carried out*

In this case customs authorities shall take into account the AEO status. If there are no other circumstances that can prevent it, customs authorities have to allow that the control is carried out in the place chosen by the AEO. These are situations where the status of the AEO and the knowledge that customs authorities have, can be used as a benefit, not enjoyed by other operators.

*- due to his or her business activities an AEO needs to use that option on a permanent basis and in combination with all the other 'possibilities' provided under the entry into declarant's records with a waiver of the obligation for the goods to be presented provided under Article 182 (3) UCC.*

In this case the status of an AEO is not enough to allow the economic operator automatic use of this simplification and permanent clearance of the goods in his or her premises. Although the AEOC status is required to have access to that simplification, a separate application is needed for this authorisation.

### **1.III.6. Indirect benefits**

It is important to highlight that, in addition to the direct benefits provided for in the legislation, an AEO may also benefit from advantages that are not directly linked to the customs side of his or her business. Although they are considered as 'indirect' benefits and therefore not explicitly reflected in the legislation, they are important as they may have a highly positive effect on the overall business of the AEO.

Some examples of indirect benefits are presented in the following subchapters.

#### **1.III.6.1. Recognition as a secure and safe business partner**

An AEO who meets the security and safety criterion is considered to be a secure and safe partner in the supply chain. This means that the AEO does everything in his or her power to reduce threats in the supply chains where he or she is involved. The AEO status, including the possibility to use the AEO logo enhances his or her reputation. While it is not necessary to work only with AEOs, the status of an AEO will have a positive influence when new business relationships are established. It is to be noted that operators can check the list of AEOs who have given their consent for the publication of their data on the TAXUD website:

[http://ec.europa.eu/taxation\\_customs/dds2/eos/aeo\\_home.jsp?Lang=en](http://ec.europa.eu/taxation_customs/dds2/eos/aeo_home.jsp?Lang=en)

#### **1.III.6.2. Improved relations with Customs and other government authorities**

The established partnership during the authorisation process and continuous cooperation will help to better understand each other and find jointly tailored solutions beneficial for both sides.

An AEO should have a designated contact point in the customs authority to which it can address its questions. The contact point might not be able to provide all answers on all questions but would guide the AEO on how to best proceed and who to further contact if necessary.

The AEO status is gaining recognition and importance in many areas. Currently, there are a number of certificates or authorisations in other policy areas for which the requirements are either one or more of the AEO criteria or directly the AEO status.

[Part 4 Section II](#) of these Guidelines includes detailed information on the exchange of information between customs and other government authorities.

#### **1.III.6.3. Other indirect benefits**

The AEO approach helps economic operators to analyse in detail all their related international supply chain processes. The activities of all concerned departments are generally assessed during the preparation of the AEO application. In most cases efficiency and cooperation between these services are optimised in order to obtain more transparency and visibility of the supply chain.

Investments 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 organisational 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 service;
- improved customer loyalty;
- improved inventory management
- improved employee commitment;
- reduced security and safety incidents;
- lower inspection costs of suppliers and increased co-operation;
- reduced crime and vandalism;
- improved security and communication between supply chain partners.

The following table summarises the different benefits available:

<b>Benefit</b>	<b>AEOC</b>	<b>AEOS</b>	<b>Reference</b>
Easier admittance to customs simplifications	X		Art. 38 (5) UCC
Fewer physical and document-based controls - related to security & safety - related to other customs legislation	X	X	Art. 24 (1) UCC DA Art. 38 (6) UCC
Prior notification in case of selection for physical control (related to safety and security)		X	Art. 24 (2) UCC DA Art. 38 (6) UCC
Prior notification in case of selection for customs control - related to security & safety - related to other customs legislation	X	X	Art. 24 (3) UCC DA Art. 38 (6) UCC
Priority treatment if selected for control	X	X	Art. 24 (4) UCC DA Art. 38 (6) UCC
Possibility to request a specific place for customs controls	X	X	Art. 24 (4) UCC DA Art. 38 (6) UCC
Indirect benefits	X	X	

Mutual Recognition with third countries		X	MRA-Agreements Art. 38 (7) UCC
---	--	---	-----------------------------------

#### **Section IV – Cooperation between customs and other government authorities**

Cooperation with other competent authorities and alignment of programmes have been identified and recognised as a key element for the further development of a robust AEO programme. It is to ensure global supply chain security and to avoid duplication of efforts and costs for authorities and economic operators.

As such it has been incorporated since the beginning at an international level in the WCO SAFE as well as in the EU legislation.

At EU level work has been initiated in a number of areas (e.g. aviation security, maritime, export controls, etc.) with a view to identify synergies and to avoid duplication of administrative burden.

The EU Strategy and Action Plan for customs risk management and in particular the inclusion of a specific objective related to interagency cooperation and information sharing between customs and other authorities had a crucial role in this area.

Besides, there are a number of certificates or authorisations in other policy areas for which the requirements are either one or more of the AEO criteria, or directly the AEO status:

- civil aviation legislation<sup>7</sup>

If a holder of an AEOS applies for the status of a Regulated Agent (RA) or a Known Consignor (KC), the respective security requirements are deemed to be met to the extent that the criteria for issuing the AEO status are identical or correspond to those for RA or KC status. The same principle applies vice versa.

In case of an Account Consignor (AC), holders of an AEOS do not need to sign the declaration of commitments 'account consignor', and are recognised as AC by the regulated agent, provided that all other requirements established by the Union legislation in the field of aviation security are met.

- Approved Economic Operator (APEO)<sup>8</sup>

For economic operators dealing with fishery products and catch certificates it is possible to apply for the status of an APEO. APEO should be eligible to use simplified procedures regarding the import of fishery products into the EU.

<sup>7</sup> Commission Implementing Regulation (EU) 2015/1998

<sup>8</sup> Commission Regulation (EC) No 1010/2009 of 22 October 2009 laying down detailed rules for the implementation of Council Regulation (EC) 1005/2008 establishing a Community system to prevent, deter and eliminate illegal, unreported and unregulated fishing

For issuing the status of an APEO it is mandatory to have an AEO status as laid down in the relevant regulations. Besides, if the APEO applicant is holder of an AEOS authorisation, the application process is simplified.

- Others

Security and safety is gaining in significance and importance for different stakeholders. The AEO status is one of the biggest security initiatives worldwide and attracting increasing attention.

At the same time, certificates and authorisations granted by customs or other government authorities facilitate the authorisation procedure.

**See also [Part 3.III.4.2. Certificates/authorisations granted by customs or other government authorities.](#)**

## **Section V - Mutual recognition**

For several years, the WCO and customs administrations set the target to enhance the security of international supply chains while providing increased facilitation for secure and reliable economic operators. The WCO SAFE Framework of Standards to Secure and Facilitate Global Trade encourages customs administrations to agree on the mutual recognition of AEO and security measures.

Strengthened cooperation between trading partners in terms of security and trade facilitation has been playing an important role in the EU. Mutual recognition of AEO status is a key element to strengthen and assist end-to-end security of supply chain and to multiply benefits for traders.

Mutual recognition entails that one customs administration in one country

- recognises the AEO authorisation issued under the other programme and
- agrees to provide substantial, comparable and, where possible, reciprocal benefits/facilitations to the mutually recognised AEOs.

Benefits from mutual recognition, amongst others, include:

- Fewer controls - The status of the trade partnership programme participant is recognised by both programmes and it is used as a risk-assessment factor in the automated targeting systems.
- Risk Management - Customs administration can identify reliable traders and focus their controls on consignments of unknown/unreliable traders

Detailed information on Mutual Recognition and its implementation is included in [Part 6 of these Guidelines.](#)

## Section VI – The AEO Logo

Authorised Economic Operators are entitled to use the AEO logo:



The AEO logo is copyrighted by the EU.

The logo is provided by the ICA and is not freely available for downloading. The ICA should provide it together with clear instructions on when and how to use it.

The AEO logo can be used under the following conditions:

- the right to use the logo is on condition of having a valid AEO authorisation;
- only the holder of an AEO authorisation can use the logo;
- the AEO must stop using it as soon as its AEO status is suspended or revoked;

Any abuse will be pursued according to EU law.

## **PART 2, AEO criteria**

### **Section I - Compliance with customs legislation and taxation rules, including no records of serious criminal offences relating to the economic activity of the applicant**

#### **2.I.1. General**

Article 39 (a) UCC requires the absence of any serious infringement or repeated infringements of customs legislation and taxation rules, including no record of serious criminal offences relating to the economic activity of the applicant. Furthermore Article 24 UCC IA considers this criterion as fulfilled if over the last three years no serious infringements of customs legislation and taxation rules have been committed or repeated and the applicant have had no record of serious criminal offences relating to his or her economic activity. In this context Article 24 UCC IA distinguishes between natural and not natural persons:

Where the applicant is a natural person, the above mentioned conditions are to be fulfilled by

- (a) the applicant and,
- (b) where applicable, the employee in charge of the applicant's customs matters.

Where the applicant is not a natural person, the criterion is to be fulfilled by

- (a) the applicant and
- (b) the person in charge of the applicant or exercising control over its management and
- (c) the employee in charge of the applicant's customs matters.

A definition of customs legislation is included in Article 5 (2) UCC. "Taxation rules" is to be understood in a broader perspective, not only those taxes related to the import and export of goods (e.g. VAT, company taxation, excise duties etc.). On the other hand, 'taxation rules' should be limited to taxes that have a direct relation to the economic activity of the applicant.

The record of compliance with customs legislation and taxation rules may be considered as appropriate if the customs authority competent to take the decision, considers an infringement to be of minor importance, in relation to the number or size of the related operations, and the customs authority has no doubt as to the good faith of the applicant.

If the person exercising control over the applicant is established or resides in a third country, or if the applicant has been established for less than three years, the customs authorities shall assess the compliance with that criterion on the basis of the records and information that are available to it.

The following common specific circumstances are recommended to be taken into account in the evaluation of the infringement by the competent customs authorities throughout the EU:

- the assessment of the compliance should cover all customs activities of the applicant including all relevant taxation elements and considering the record of serious criminal offences relating to the economic activity of the applicant;
- the term "infringement" shall refer not only to the acts which are discovered by customs authorities on the occasion of checks carried out at the time when the goods are introduced into the customs territory of the Union, or being placed under a customs procedure. Any infringements of the customs legislation, taxation rules or criminal

laws discovered on the occasion of any post clearance control carried out at a later stage, shall also be considered and assessed, as well as any infringements that could be discovered through the use of other customs authorisations and any other source of information available for customs authorities;

- infringements made by freight forwarders, customs agents or other third parties acting on behalf of the applicant shall be also taken into account. The applicant should show evidence that appropriate measures have been put in place to ensure the compliance of persons acting on its behalf such as clear instructions to those parties, monitoring and checking of the accuracy of declarations and remedial action when errors occur;
- failures to comply with domestic non-customs or non-taxation legislation by the applicant in the different Member States are not to be ignored, although in this case those failures should be considered in the light of the trader's good faith and relevance for its customs activities;
- where penalties related to a specific infringement are revised by the competent authority following an appeal or review, their assessment of the seriousness of the infringement should be based on the revised decision. Where the penalty for an infringement is withdrawn in full by the competent authority, the infringement shall be deemed not to have taken place.

Before a decision is taken if the criterion of record compliance is fulfilled, it is necessary to compare the full number of infringements committed by the applicant to the full number of customs operations carried out by the applicant in the same period of time to establish appropriate ratios. In this context the different types of activities are to be considered in terms of the number and volume of the customs declarations and operations made by the applicant.

### **2.I.2. Infringements of minor importance**

Infringements of minor importance are those acts that, even if there was an actual infringement of any aspect of the customs legislation and taxation rules, are not sufficiently important to be considered as a risk indicator with regard to the international movement of goods, security issues or demandable customs debt.

In order to establish what may be regarded as an infringement of minor importance, the first point to be observed is that each case is different and should be treated on its own merits against the compliance history, nature of activities and size of the economic operator concerned. If a decision is taken that the infringement may be regarded as of minor importance, the operator must show evidence of intended measures to be undertaken to reduce the number of errors occurring in his or her customs operations.

The following indicative checklist may assist customs authorities when evaluating whether an infringement could be regarded of minor importance:

- there must be no deliberate fraud intended;
- infringements should be looked at on a cumulative basis but relative to the total volume of operations;
- establishment of whether the infringement was an isolated or sporadic act by one person within the general organisation of the company;
- the context of the infringement should always be considered;



- the internal controls systems of the applicant should be in place and it should be taken into account if the offences have been detected by the applicant himself as a result of its own internal checks and whether they were immediately notified to customs authorities;
- if the applicant has taken immediate measures to correct or avoid those acts in the future;
- nature of the infringement – the customs authorities should take into account the type and size of the infringement. Some errors can be defined as ‘of minor importance’ because they have no impact on the amount of customs duties to be paid, for example an incorrect classification between two commodities with the same duty rate and no difference between the other measures applicable to them (for example prohibitions and restrictions). Other infringements may affect the amount of duties to be paid, but the difference is not considered to be significant in terms of the number and volume of the declarations made by the applicant.

If as a result of the evaluation the infringements committed have been considered as being of minor importance, the record of compliance should be considered as appropriate.

Taking the above mentioned into consideration, and providing that in each case analysed there are no other circumstances to be taken into account, the following infringements could be given as examples of customs infringements of minor importance:

- failures which are considered to have no significant effect on the operation of a customs procedure as defined in Article 5 (16) UCC;
- minor failure to comply with the maximum period allowed for goods to have the status of goods in temporary storage or any other time-limits applicable to goods under any suspension customs procedure, i.e. inward processing or temporary admission, without this affecting the correct determination of the demandable customs debt;
- isolated, non-recurring, errors incurred by the operator when completing the data included in the customs declarations filed, providing such errors did not result in an incorrect assessment of the demandable customs debt.

As regards infringements of minor importance regarding taxation rules definition established by the competent taxation authority is to be taken into account.

### **2.I.3. Repeated infringements**

In case of infringements which could be initially considered as minor or being of minor importance, the customs authorities should establish whether there has been a repetition of infringements that are identical in nature. In this case customs authorities should analyse whether that repetition is the result of the action of one or several particular persons within the applicant's company, or if it is the result of structural deficiencies within the applicant's systems. The customs authorities should also detect whether the type of infringement is continuing to occur or the cause of the infringement has been identified by the applicant and addressed and will not happen again in the future. On the contrary, in case the infringement happens again in different periods of time, this could be an indication for an inadequate internal management of the company as far as the adoption of measures to prevent the repetition of such infringements is concerned.

As regards repeated infringements regarding taxation rules definition established by the competent taxation authority is to be taken into account.

## 2.I.4. Serious infringements

The following elements should be taken into account when assessing serious infringements:

a) Deliberate Acts

deliberate intent or fraud, which means proven to be with full knowledge and intention, by the applicant, the person in charge of the applicant or exercising control over its management or the person in charge of the applicant's customs matters should be considered as more serious infringement than the same case under other circumstances, even if the nature of the error could be considered to be 'of minor importance';

b) Nature of the infringement

Where an infringement is of such character that it can be considered a serious infringement of the customs legislation and taxation rules and which requires the imposition of a significant penalty or referral to the criminal proceedings;

c) Obvious Negligence

the European Court of Justice (ECJ)<sup>9</sup> has set out the following three factors that should be taken into account in assessing whether an act committed by the economic operator business has been obviously negligent: the complexity of the customs legislation, the care taken by the business and their experience. Where the customs authorities have established that the business has been obviously negligent, this can be an indicator that the infringement may be deemed to be serious;

d) Serious risk indicator with regard to security or safety or customs, taxation rules and criminal offences relating to the economic activity

Serious infringements could also be those that, even without the aim of the applicant of committing a fraud, are so important to be considered a serious risk indicator with regard to security and safety or customs, taxation rules and criminal offences relating to the economic activity.

Taking the abovementioned into consideration, and providing that in each case analysed individually there are no other circumstances which should be taken into account, the following infringements could be given as examples of serious infringements:

- customs legislation
  - smuggling;
  - fraud, for example deliberate misclassification, undervaluation and overvaluation or false declared origin to avoid payment of customs duties;
  - infringements related to Intellectual Property Rights (IPR);
  - fraud regarding antidumping regulation;
  - Infringements relating to prohibitions and restrictions;
  - counterfeiting;
  - any other offence related to customs requirements.

---

<sup>9</sup> Jurisprudence of the European Court of Justice on obvious negligence : "C- 48/98 Söhl & Söhlke (1999)"

- taxation rules
  - tax fraud;
  - tax evasion;
  - criminal offences relating to excise duties, for example illegal manufacturing or refining of mineral oil and subtraction;
  - VAT fraud, including the intra-union movements of goods.
- serious criminal offences relating to the economic activity of the applicant
  - bankruptcy (insolvency) fraud;
  - any infringement against health legislation, for example placing on the market goods of unsafe nature;
  - any infringement against environmental legislation, for example illegal cross-border movement of hazardous waste;
  - fraud related to dual-use regulation;
  - participation in a criminal organisation;
  - bribery and corruption;
  - fraud;
  - cybercrime;
  - money laundering;
  - direct or indirect involvement in terrorist activities (e.g. carrying out any business or other activities that promote or assist the internationally recognised terrorist groups);
  - direct or indirect involvement in promoting or assisting illegal migration to the EU.

**Section II - Satisfactory system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls**

**2.II.1. General**

In order to enable the customs authorities to establish that the applicant has a high level of control of his or her operations and of the flow of goods, by means of a system of managing commercial and, where appropriate, transport records which allows appropriate customs controls, the applicant shall fulfil all the requirements laid down in Article 25 UCC IA.

The following general considerations should be taken into account regarding the verification of this particular criterion:

- it should be checked against all the customs activities of the applicant;
- customs authorities should use all available information and knowledge of any authorisations already granted to the applicant. In general, there should be no need for this part of the business to be rechecked if the previous audit was carried out recently and there have been no subsequent changes. However, it has to be ensured that all different aspects/conditions have been covered during that previous audit;
- it is recommended that part of the verification is done on the spot while visiting the company;
- whilst the audit is being done at the applicant's premises there are several crucial elements to be considered:
  - verification that the information that has been given in the application and the other documents is correct and that the routines/procedures described by the applicant are

documented and implemented in practise;

- transaction tests to ensure that there is an audit trail in the records;
- verification that the IT system used is reasonably protected against intrusion, manipulation and also that historic events are logged in the system so that changes can be monitored if necessary.

With regard to the check of the specific requirements listed in Article 25 (1) UCC IA, customs authorities have to take always into account the specific nature/business and size of the operator, however, bearing in mind also a number of common considerations.

## **2.II.2 Condition of satisfactory system of managing commercial and transport records**

a) Article 25 (1) (a) UCC IA requires that *"the applicant maintains an accounting system which is consistent with the generally accepted accounting principles applied in the Member State where the accounts are held, allows audit-based customs control and maintains a historical record of data that provides an audit trail from the moment the data enters the file"*.

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 track the life cycle of operational activities of the applicant, in this respect related to the flow of consignments, goods and products coming in, being processed and leaving the company premises. Many businesses and organisations require an audit trail in their automated systems for security reasons. It is important to combine the checks done in the business system with checks done for security and safety. For security and safety it is important that where appropriate the information in the business system reflects the physical movement of consignments, goods and products and that should be a part of the verification. It is also important that where appropriate the information in the business system reflects the flow of consignments, goods and products and the measures taken with a view to their security and safety at the different stages in the international supply chain where the AEO is involved. Transaction tests should reflect both these issues when done and also make sure that the company follows the given routines at all times. The audit trail maintains a historical record of the data that enables the user to trace a piece of data from the moment it enters the data system to the time it leaves.

b) Article 25 (1) (b) UCC IA requires that *"records kept by the applicant for customs purposes are integrated in the accounting system of the applicant or allow cross checks of information with the accounting system to be made"*.

Some economic operators use an Enterprise Resource Planning (ERP) software to map their core business processes. The records kept for customs purposes can be integrated or linked electronically in this ERP.

There is no need, especially for SMEs, to use one single integrated system but to allow the possibility of cross checks between customs records and the accounting system. This can be achieved via an automated link, interface or even cross references in both systems or documentation.

c) Article 25 (1) (c) UCC IA requires that *"the applicant allows the customs authority physical access to its accounting systems and, where applicable, to its commercial and transport records"*.

see point d) below.

d) Article 25 (1) (d) UCC IA requires that *“the applicant allows the customs authority electronic access to its accounting systems and, where applicable, to its commercial and transport records where those systems or records are kept electronically.”*

Access to company's records is defined as the possibility of getting the required information, no matter where the data is physically stored. Required information includes the company's records as well as other relevant information, which is needed to perform the 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;
- **Portable data storage devices:** a copy of the required information is handed out on CD-ROM or similar media. The situation is appropriate when bigger quantity of information is involved and data processing is needed;
- **on-line access:** through the company's computer system in case of site visit, using electronic channels for exchange of data, including the internet.

No matter which way data is accessible, customs authorities should have the possibility of data interrogation and analysis (e.g. is able to work on the data). It is also important, that the data provided are always up to date.

For this particular condition the nature of SMEs shall be taken into account. For example, while all applicants seeking an AEO will have to demonstrate a good record-keeping system to facilitate audit-based customs controls the way it is achieved may vary. For a large applicant it might be necessary to have integrated electronic record-keeping system directly facilitating for customs authorities to audit while for an SME having only a simplified and paper-based system of record-keeping might be enough if it allows customs to do the relevant controls.

e) Article 25 (1) (e) UCC IA requires that *“the applicant has a logistical system which identifies goods as Union or non-Union goods and indicates, where appropriate, their location”*.

It has to be assessed how the non-Union goods or goods subject to customs control are distinguished from the Union goods. According to Article 25 (2) UCC IA AEOS are waived from this condition. The reason is that the provisions related to security and safety do not differentiate between Union or non-Union goods. The security requirements apply to all goods entering or leaving the customs territory of the Union, irrespective of their status.

As far as SMEs are concerned, the fulfilment of this condition may be regarded as satisfactory if the distinction between Union and non-Union goods can be done by means of a simple electronic file or paper records, provided that they are managed and protected in a secure way.

f) Article 25 (1) (f) UCC IA requires that *“the applicant has 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 has internal controls capable of preventing, detecting and correcting errors and of preventing and detecting illegal or irregular transactions”*.

It has to be taken into account that no 'standard rule' for administrative organisation exists. The most important to be demonstrated by the applicant is that the administrative organisation that is in place is suitable, taking into account the applicant's business model, for the management of the flow of goods and that there is an adequate system for internal control. Therefore, the use of any 'quantitative thresholds' i.e. minimum number of staff etc. is not appropriate.

Notwithstanding the above, written procedures and working instructions with clear description of the processes, the competences and representation in case of absence are expected and to be properly implemented. For micro and small businesses such expectations can also be met by other appropriate measures which are to be demonstrated to the ICA.

Internal control procedures impact not only everyday functioning of the department responsible for the operations covered by customs legislation, but also all the services involved in managing those activities related to the international supply chain where the applicant is involved in. Examples for internal control are various and lead from a simple "two-man rule" to complex electronical plausibility checks.

Every irregularity in the administration including customs infringements can be an indicator that the internal control system is not being effective. In this perspective every customs infringement has always to be scrutinised also with respect to this condition in order to take measure to improve the internal control system and therefore avoiding the repetition of the infringement.

g) Article 25 (1) (g) UCC IA requires that, *"where applicable, the applicant has satisfactory procedures in place for the handling of licenses and authorisations granted in accordance with commercial policy measures or relating to trade in agricultural products"*.

Based on the information provided in the [SAQ](#) and any other information available to customs authorities, it is important to identify in advance if the applicant trades in goods that are subject to economic trade licences (e.g. 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. If necessary the practical application of these routines and procedures has to be verified on the spot.

In case of trade with specific goods subject to any licences issued by other competent authorities it is advisable that customs authorities consult them for any feedback/background information on the applicant.

h) Article 25 (1) (h) UCC IA requires that *"the applicant has satisfactory procedures in place for the archiving of its records and information and for protection against the loss of information"*.

Procedures for archiving and retrieving of the applicant's records and information have to be assessed, including on what kind of media and in which software format the data is stored, and whether the data gets compressed and at what stage. If a third party is used, the relevant arrangements have to be clear, in particular the frequency and location of any back-up and archived information. An important aspect of this condition is related to possible destruction or loss of relevant information. Thus, it should be checked whether a safety plan exists,

including action points describing the measures to be taken in case of incidents and whether it is regularly updated. Any back-up routines when computer systems don't work should be checked.

i) Article 25 (1) (i) UCC IA requires that *"the applicant ensures that relevant employees are instructed to inform the customs authorities whenever compliance difficulties are discovered and establishes procedures for informing the customs authorities of such difficulties"*.

The applicant should have procedures in place for notifying customs in case of customs compliance difficulties and also an appointed contact person responsible for notifying the customs authorities. Formal instructions should be addressed to employees involved in the supply chain in order to prevent possible difficulties to comply with customs requirements. All identified difficulties should be reported to the appointed responsible person (s) and/or his or her replacement(s).

For that, it is helpful, that the contact details of the appointed person are clearly visible for the staff who is dealing with the goods as well as for those dealing with the related information (e.g. posted on a black board and/or next to the telephone).

To identify which kind of information is to be reported from the economic operator, a list of examples is included in [Annex 4 of these Guidelines](#).

j) Article 25 (1) (j) UCC IA requires that *"the applicant has appropriate security measures in place to protect the applicant's computer system from unauthorised intrusion and to secure the applicant's documentation"*.

Procedures for protecting the computer system from unauthorised intrusion and securing data have to be in place. This may include how the applicant controls access to the computer systems through the use of passwords, protects against unauthorised intrusion, for example through the use of firewalls and anti-virus protection and how the applicant files and ensures the secure storage of documents. Those security measures should not only cover hardware kept in the premises of the applicant's company, but also mobile devices allowing access to the applicant's data (e.g. hard drive encryption for laptops, passwords for smartphones).

Personal Computers should be automatically locked after a short period of inactivity. Furthermore, computers should have a regular updated antivirus programme and a firewall installed. The configuration of the computer should be centrally administered.

Servers should be placed in locked rooms with controlled limited access to relevant staff.

k) Article 25 (1) (k) UCC IA requires that, *"where applicable, the applicant has satisfactory procedures in place for the handling of import and export licences connected to prohibitions and restrictions, including measures to distinguish goods subject to the prohibitions or restrictions from other goods and measures to ensure compliance with those prohibitions and restrictions"*.

The handling of import and/or export licenses connected to prohibitions and restrictions was previously included under the criterion on safety and security and as such limited to the AEOS status to prevent misuse and unlawful delivery of security and safety sensitive goods. It has to be seen in close context to Article 25 (1) (g) UCC IA.

The addressed procedures may be/include:

- to distinguish goods subject to non-fiscal requirements and other goods;
- to check if the operations are carried out in accordance with current (non-fiscal) legislation;
- related to the handling of goods subject to an embargo;
- related to the handling of licenses;
- regarding other goods that are subject to restrictions;
- to identify potential dual-use goods and routines attached to their handling.

With respect to this condition it is crucial that the staff is aware of the importance of non-fiscal requirements, the correct classification of goods and keeping the master data up to date. Regular training or self-study of the developing legislation is mandatory for businesses dealing with above mentioned goods.

Besides it is vital for the economic operator to contact the competent national authorities for non-fiscal requirements if any questions arise at an early stage. This is especially for start-up companies or in case economic operators are enlarging their portfolio.

When assessing this condition, customs should consult other involved competent authorities to get as much information about the economic operators processes as possible.

## **Section III - Proven financial solvency**

### **2.III.1. General**

As indicated in Article 39 (c) UCC, an AEO has to prove that he or she has good financial standing, which enables him or her to fulfil his or her commitments with due regard to the characteristics of the type of business activity concerned. Article 26 UCC IA, which describes more precisely the expectations of the ICA with regard to the criterion set in Article 39 (c) UCC has to be read accordingly.

To check whether the applicant meets the criterion in Article 26 UCC IA the customs authorities shall take into consideration the following:

- a) the applicant is not subject to bankruptcy proceedings;*
- b) during the last three years preceding the submission of the application, the applicant has fulfilled his or her financial obligations regarding payments of customs duties and all other duties, taxes or charges which are collected on or in connection with the import or export of goods;*
- c) the applicant demonstrates on the basis of the records and information available for the last three years preceding the submission of the application that he or she has sufficient financial standing to meet his or her obligations and fulfil his or her*



*commitments having regard to the type and volume of the business activity, including having no negative net assets, unless where they can be covered.*

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

It is to be noted that the term "insolvency" within this Section of the Guidelines is 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. For this criterion the focus is more on the technical meaning of insolvency and on the possible risk that, due to its economic and financial situation, an economic operator will be unable to satisfy its debts. In this context any indications that the economic operator is unable or may in the immediate future be unable to meet its financial obligations should be carefully considered and evaluated.

### **2.III.2. Sources of information**

When considering the proven financial solvency criterion it is important that all the information is, where appropriate, considered together in order to get the full overview. One indicator should not be considered in isolation and decisions should be based on the overall position of the applicant reflecting that the main purpose is to ensure that, once granted the AEO status, the operator concerned will be able to continue to fulfil his or her obligations.

Customs authorities may rely on various sources of information to assess this criterion, i.e.:

- official records of insolvencies, liquidations and administrations;
- the record for the payment of customs duties and all other duties, taxes or charges which are collected on or in connection with the importation or exportation of goods during the last three years;
- the published financial statements and balance sheets of the applicant covering the last three years in order to analyse the applicant's ability to pay their legal debts;
- draft accounts or management accounts, in particular any interim reports and the latest cash flow, balance sheet and profit and loss forecasts approved by the directors/partners/sole proprietor, in particular where the latest published financial statements do not provide the necessary evidence of the current financial position or the applicant has a newly established business;
- the applicant's business case where the applicant is financed by a loan from a financial institution and the facilities letter from that institution;
- the conclusions of credit rating agencies, credit protection associations or any relevant public authorities' rating;
- any accessible financial information such as legal record, online databases, financial news etc.
- other evidence which the applicant may provide, for example a guarantee from a parent (or other group) company that demonstrates that the applicant is financially solvent.

### **2.III.2.1. The applicant is not subject to bankruptcy proceedings**

If the applicant is subject to bankruptcy proceedings or liquidation, the criterion of financial solvency as defined in Article 39c UCC and Article 26 (1) UCC IA is not met.

If the applicant is subject to any form of insolvency, the compliance with the above mentioned criterion has to be further explored, for instance controlled administration by a third person selected by the judge. 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 to the amount of different types of assets 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 (property, plant and equipment and other capital assets, net of depreciation), intangible assets (assets with a determined value, but which may not be realised, such as goodwill, patents, copyrights, and brand name recognition) and prepaid (expenditures for future costs or expenses, such as insurance, interest or rent) and deferred assets.

### **2.III.2.2. Payment of customs duties and all other duties, taxes and charges which are collected on or in connection with the import or export of goods**

The customs authorities can establish whether the applicant has paid or was late in paying the customs duties/taxes that are legally due to customs in the last three years. This excludes amounts that are not yet legally due or are under appeal. In case of appeal, when the relevant decision is suspended by the customs authority, it should be checked whether a guarantee covering the customs debt was provided. If it has not been provided as requested by Article 45 (3) UCC, the report justifying this release should be consulted.

Generally, where the applicant has not paid amounts that are legally due, the proven solvency criterion will not be met. However the reasons for the non-payment or late payment should be examined to determine whether there are acceptable mitigating circumstances. Examples of such mitigating circumstances might include:

- a short term or one-off cash flow or liquidity issue where the overall financial status and reliability of the applicant is not in doubt;
- where the applicant was late in making a payment because of an administrative error, rather than any underlying solvency issue, this should not affect their compliance with this criterion.

There is a possibility for a company to apply for payment facilities as provided for in Articles 111 to 112 UCC. The existence of such deferral applications should not result automatically in the applicant being regarded as unable to pay, and thus being denied the AEO status.

However, apart from any payment facilities granted, in the other cases the amounts due have to be paid within the periods legally prescribed. The obligations stipulated by the provisions of Title III UCC DA shall be considered related not only for the payment itself, but also regarding the time-limits for the payment. Any non-compliance with these time-limits should be considered with a view to the overall customs compliance of the applicant.

Where applicable, if the company has asked for reimbursements of customs duties or taxes and charges that are related with the import or export of goods, the evidence of these reimbursements might be further examined by the ICA.

### **2.III.2.3. The applicant can demonstrate sufficient financial standing to meet his or her obligations and fulfil his or her commitments**

The customs authorities can establish whether the applicant is able to meet his or her legal debts to third parties by checking the applicant's full sets of financial statements due in the last three years taking into account:

- where required by company law, the accounts have been filed within the time-limits laid down in that law. Failure to file the accounts within the required time-limits is an indicator that the business may have problems with their records or be in financial difficulties. Where the time-limits have not been met, the customs authorities should make further enquiries to establish the reasons;
- any audit qualifications or comments about the continuation of the business as a going concern by for example the auditors or directors. Where internal or external auditors have doubts about the solvency of a business, they may either qualify the accounts or record their reservations in their reports. Similarly the directors may also, exceptionally, make such a comment. Where this is the case the customs authorities should investigate the reason for the comment with the auditor or director and consider its significance for the business;
- any contingent liabilities or provisions. Significant contingent liabilities will give an indication of the applicant's ability to pay future debts;
- any additional financial documents such as income statement or cash flow can be used to assess the financial standing of the company;
- any ratio analysis, if available (e.g. current ratio (current assets divided by current liabilities) which measure the company's liability to meet present obligations from its liquid assets);
- any other conclusions provided by financial or research institutions ;
- other indicators that could be interesting to be assessed, such as whether a company has been subject to important strikes, whether a company has lost main projects in which it was involved or whether a company has lost major and key suppliers.

If the applicant uses a special procedure such as Union transit or customs warehousing in general, the applicant should already have demonstrated it has sufficient financial resources to cover his or her obligations under these procedures. For example for Union transit if the applicant has been already given an authorisation for reduced amount of the comprehensive guarantee or guarantee waiver this has to be taken into account by customs authorities as he or she has already demonstrated sufficient financial resources to meet any obligations that might arise during the use of the transit procedure. In such cases and if the applicant has no other customs related activities, there is no need for customs authorities to re-examine or duplicate checks that have already been carried out.

#### **2.III.2.4. The applicant has no negative net assets unless where they can be covered**

The customs authorities should examine two key indicators in the financial statements and balance sheets to assess the proven solvency criterion: the net current assets position (current assets minus current liabilities) and net assets position (total assets minus total liabilities).

- the net current assets position is an important indicator of whether the applicant has sufficient capital available to conduct its day to day operations. The customs authorities should compare the net current assets over the three sets of accounts to identify any significant trends over the three years and examine the reasons for any changes, for example, if the net current assets move from a positive to a negative situation or the net current assets are becoming increasingly negative. This may be due to the impact of falling turnover or adverse trading conditions or increased costs. The customs authorities should assess whether this is due to short term factors or whether it affects the long term viability of the business;
- the net assets position is an important indicator of the longer term viability of the applicant and its ability to pay its debts. It is expected that a business should have positive net assets to meet the proven financial solvency criterion. Where the net assets include significant intangible assets such as goodwill the customs authorities should consider whether these intangible assets have any real market value. The customs authorities should also take into account the nature of the business and its lifespan. In some circumstances 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. Similarly new businesses may often trade at a loss and with negative net assets when they are first set up whilst they are developing their products or building up their customer base, before they start to receive returns on their investment in subsequent years. In these circumstances negative net assets may not be an indicator on which to place high emphasis that a business is unable to pay its legal debts.

The latest draft accounts or management accounts between the latest signed financial statements and the current date should also be reviewed to determine whether there have been any significant changes to the financial position of the applicant that may impact on its proven financial solvency.

In case of concerns the applicant can take a number of actions to improve the net assets position. For example additional capital can be raised through a share issue. For multinational companies negative net assets may often arise from inter-group transactions and liabilities. In these circumstances liabilities may often be covered by a guarantee from the parent (or other group) company.

#### **2.III.3. Finance from a loan from another person or a financial institution**

If the applicant is financed by a loan from another person or financial institution, customs authorities can also require a copy of the applicant's business case and the bank facilities letter or equivalent document. The customs authorities should compare the business case and/or loan document with the latest cash flow, balance sheet and profit and loss forecasts to ensure the applicant is operating within its approved overdraft facility and performing in line with its forecast at the time of completing its business case. Where there are significant differences the reasons should be investigated.

However, the customs authorities may require further evidence such as an undertaking from the lender or a bank facilities letter and establish the period of the loan and any terms and conditions attached to it. The customs authorities should check the position recorded in the accounts is consistent with the undertaking or bank facilities letter. If the applicant is a sole proprietor or partnership and personal assets are being used to support the solvency of the business the customs authorities should obtain a list of any personal assets and satisfy themselves that the list is credible.

The company may be required to provide additional information regarding a loan, for instance the name of the creditor, the purpose of the loan and its conditions. This information should be checked and compared with other financial documents (e.g. balance sheets, Profit & Loss statement) in order to assess the global financial situation of the economic operator.

#### **2.III.4. Letters of comfort and guarantees from parent (or other group) companies**

Letters of comfort are documents usually issued by a parent (or other group) company acknowledging the approach of a subsidiary company's attempt for financing. Letters of comfort may be found where the subsidiary company has negative net assets and are used to support the directors' opinion and evidence the auditor's opinion that the company has adequate financial resources to continue to operate as a going concern. They may be limited to a specific period of time. They represent a written statement of intent to continue with financial support to the applicant company but are not necessarily legally binding.

When judging the proven financial solvency of a subsidiary, it should be taken into account that a subsidiary company may operate under a guarantee from the parent company and the customs authorities could look into the accounts of that parent company providing support to ensure it has the facilities to do so.

It is to be noted that letters of comfort are often not legally binding contractual agreements and therefore do not constitute a legally enforceable guarantee. Where the applicant is dependent on the financial support of a parent (or other group) company to meet the proven financial solvency criterion the customs authorities should, where appropriate, ensure the support is provided in a legally binding, contractual agreement. If a guarantee is required as evidence of support from the parent (or other group) company it must be legally binding according to the national legislation of the Member States where it is accepted, otherwise it cannot be taken into account in assessing compliance with the criterion. To constitute a legally binding, contractual agreement it must contain an undertaking to irrevocably and unconditionally pay the liabilities of the subsidiary. Once signed it has to be the legal responsibility of the signatory to pay any customs debts that are not paid by the applicant.

#### **2.III.5. Applicants established in the EU for less than three years**

Where the applicant has been established in the EU for less than three years, it will not be possible to carry out the same depth of financial checks as for longer established businesses. The absence of information about the financial history of the applicant increases the level of risk for the customs authorities. In these circumstances proven financial solvency will be judged, according to Article 26 (2) UCC IA, on the basis of records and information that are available at the time of the application. This could include any interim reports and the latest

cash flow, balance sheet and profit and loss forecasts provided by the directors/partners/sole proprietor.

The customs authorities should also be alert to applications from businesses that have gone into liquidation to avoid their liabilities and started up again under a different name. Where the customs authorities have information showing that the persons controlling the applicant have had previous control over a business that falls into this category and the new business is to all intents and purposes the same business as the previous legal person which went into liquidation, this information can be used to challenge whether the applicant has a sufficiently good financial standing to satisfy the proven financial solvency criterion.

Customs authorities on the other hand should consider the case where the applicant had been established for less than three years as a result of a corporate re-organisation but the economic activity remains the same. In order to evaluate this criterion, customs authorities could consider the company accounts, management accounts, financial statements or any other relevant documents of the pre-existing company provided that the economic activity has not changed.

## **Section IV - Practical standards of competence or professional qualifications directly related to the activity carried out**

### **2.IV.1. General**

Article 39 (d) UCC requires an additional criterion for the AEOC authorisation relating to practical standards of competence or professional qualifications directly related to the activity carried out. According to Article 27 UCC IA, the criterion is considered to be fulfilled if any of the following conditions are met:

- *The applicant or the person in charge of the applicant's customs matters complies with one of the following practical standards of competence:*
  - *a proven practical experience of a minimum of three years in customs matters;*
  - *a quality standard concerning customs matters adopted by a European Standardisation body.*
- *The applicant or the person in charge of the applicant's customs matters has successfully completed training covering customs legislation consistent with and relevant to the extent of his or her involvement in customs related activities, provided by any of the following:*
  - *a customs authority of a Member State;*
  - *an educational establishment recognised, for the purposes of providing such qualification, by the customs authorities or a body of a Member State responsible for professional training;*
  - *a professional or trade association recognised by the customs authorities of a Member State or accredited in the Union, for the purposes of providing such qualification.*

*Where the applicant uses a contracted person, the criterion shall be considered to be fulfilled if the contracted person is an AEOC.*

All concrete possibilities to demonstrate compliance with any of the two conditions (practical standards of competence or professional qualifications) are equally sufficient and can be chosen by the applicant; however they have to reflect the specific involvement of the applicant in customs related activities and his or her role in the supply chain, his or her status and the business organization process set up in the applicant's company.

It should be noted that the person in charge of the applicant's customs matters can be an employee of the applicant or a contracted person. The applicant has to prove that the contracted person is actually the one in charge of the applicant's customs matters.

## **2.IV.2. Practical Standards**

### **2.IV.2.1. Proven practical experience of a minimum of three years in customs matters**

#### **Scope**

Practical standards means that the applicant or the person in charge of the applicant's customs matters must demonstrate that they have acquired experience in dealing with customs matters. Purely theoretical knowledge of the customs legislation is not sufficient. Nevertheless, the experience of minimum of three years in customs matters does not refer to the immediate period before submitting an application, but it can be spread over a longer timeframe. The relevance of the experience gained over any period would have to be assessed by the ICA.

The three years standing practice shall also take into account the role of the applicant in the supply chain as referred to in [chapter 1.II.4. of these Guidelines](#), for example:

- An exporter/ manufacturer as defined in [chapter 1.II.4. \(b\)/\(a\) of these Guidelines](#), can prove the three years of practical experience being a holder of an authorisation for the entry into the declarant's records with the waiver of the obligation for the goods to be presented for the use of the export customs procedure for a period of at least three years or performing the role "exporter" in a normal export customs procedure over the last three years.
- A customs agent as defined in [chapter 1.II.4. \(e\) of these Guidelines](#) can prove the three years of experience by having an authorisation on customs simplifications (where applicable) or by being contracted in this area for a period of at least three years.
- A carrier as defined in [chapter 1.II.4. \(f\) of these Guidelines](#) can demonstrate his or her practical experience if he or she has been holder of an authorisation for a simplified procedure in relation to customs transit or an authorised consignee under the TIR Convention under the last three years or has undertaken contract and issued transport documents as well as summary declarations during the last three years.

#### **Verification of the fulfilment**

It is to be noted that the verification of the fulfilment only relates to the duration of the professional experience. Infringements or compliance deviations do not affect the 3 years professional experience, but have to be considered when examining the fulfilment of the

criterion on compliance with customs legislation and taxation rules and internal control systems addressed under [2.I.1.](#) and [2.I.2.](#) of these Guidelines.

#### **a) Applicant**

In case the person who has to comply with the condition of three years' proven practical experience in customs matters is the applicant in the form of either legal or natural person, he or she can demonstrate to meet this condition with one or more of the following possibilities:

In case of submitting an application the following alternative elements are to be taken into consideration

- Carrying out customs activities (e.g. import/export/transit) or customs formalities for three years at least. For the evaluation of the three years of experience in customs matters, the ICA should take into account the type of the business activity carried out (e.g. permanently or seasonally, few declarations but with a high value). Proof can also be established by the presence of the applicant's EORI number in box 2, 8, 14 or 50 of the customs declarations or by the payment of customs duties and/or guarantee ensured for customs rights. It should be noted that the simple presence of the applicant in one of the mentioned boxes of the customs declarations does not mean that he or she is directly involved in the performing of customs formalities. In this case it is important for customs to know if the customs formalities are directly performed by the applicant (inside the company) or by third parties (e.g. customs agents). If the latter is true, the applicant is not exempted from having to insure that the formalities are carried out properly. In other words, if the customs management/formalities are performed by third parties on an occasional basis and, therefore are not covered by the definition of contracted person, the criterion can be met by the applicant if it has an internal organisation which allows the supervision and control on the customs management/formalities carried out by the third parties.
- Being a holder of a particular authorisation granted under the UCC and related DA/IA or, until applicable, under the CCIP, for at least three years related to the customs activities carried out.
- Carrying out customs brokerage services for at least three years, proof can be established through customs declarations and all the other necessary documents; evidence of payment and/or guarantee ensured for customs rights, presence of the EORI number in box 14 of the customs declarations.
- Organising the transportation of goods in international trade on behalf of an exporter, an importer or another person, obtaining, checking and preparing documentation to meet customs requirements and/or acting as carrier and issuing its own transport contract, this can be checked by e.g. bill of lading, air waybill.

Customs authorities should use all available information and knowledge of the authorisations already granted to the applicant and the declaration submitted on the basis of their data bank and electronic systems.

Another element that customs should take into account is the official document of the applicant that clearly defines his or her economic activity and the general objective of the applicant's company (e.g. extract from official register, if applicable).



In case the applicant is established less than three years as a result of a corporate re-organisation, the customs authorities shall consider the customs activities performed by the pre-existing company provided that they are unchanged.

## **b) Person in charge of the applicant's customs matters**

### **aa) the applicant's employee in charge of customs matters**

**The criterion can also be fulfilled by the applicant's employee(s) in charge of customs matters.** The employee is the person who covers the position(s) created inside the organisation of the applicant (defined through e.g. organisational structure, functional structure, divisional structure, working instructions or other organisational measures) of a person "responsible" for customs matters, being, for instance, the person responsible for the import and export office or an employee of the office managing customs matters..

### **Scope**

**In case the person who has to comply with the condition is the applicant's employee in charge of customs matters,** there must be an employment relationship that creates a legal link between employer (applicant) and employee. This means that the employee performs, **for the applicant,** work or services on customs matters, under certain conditions in return of a remuneration. Due to this relationship, the employee does not act as a customs representative (direct or indirect) of the applicant (e.g. box 2 and 14 of the export customs declaration includes only the EORI number of the applicant/exporter). As a result, it is the applicant who is the person responsible as far as the financial and legal liability is concerned and in case of infringements of customs laws occurred in performing the duties.

It should be noted that depending on the internal organisation of the applicant, more than one employee can be in charge of the customs activities. In this case the condition has to be fulfilled by all employees in charge.

Should another employee become in charge of the applicant's customs matters, the economic operator has to inform the ICA who can evaluate the real necessity to assess the new situation on the basis of the information provided (e.g. the name of the person(s) involved in the rotation and their experience in customs matters inside the company).

### **Verification of the fulfilment:**

If the employee in charge of the applicant's customs matters is working for the applicant for less than three years, the employee can demonstrate to comply with the criterion by providing the evidence to have previously worked on relevant issues in another company. In this case the proof of compliance will have to be provided by the previous work contract or the organisational structure of the other company, by a statement from this company clearly indicating the employment status of the employee within this previous company or other means of proof held by the employee and recognised by the customs authorities. In case the applicant is an SME, especially a micro or small company (e.g. a family business), it can have a different management and organisational structure without a real distinction of the internal roles or working position. In this case the applicant's formal statement could be considered sufficient.

## **bb) A person outside the applicant**

**The criterion can be fulfilled by a person outside the applicant** only in case the managing/handling of the customs matters is outsourced.

### **Scope**

In this case the applicant is represented directly (on its own name and behalf) or indirectly (on its own behalf) by a third party regarding the customs formalities (e.g. the applicant outsources the customs formalities to a customs agent or a freight forwarder).

The criterion cannot be fulfilled by contracted persons to whom the applicant has outsourced activities other than customs related such as, for instance, information technology.

In any case there is always a contract in return of a remuneration that defines the services that the contracted person has to provide. This contract usually includes a draft set of terms and conditions. The length of the contract is determined at the outset as an integral part of the business case for the outsourcing activity.

There are different reasons to outsource the customs activities. For example SMEs often, for economic and management reasons, outsource important functions to specialised companies having a degree of technical knowledge that cannot be achieved by the applicant. Some examples of outsourcing include:

**Customs agents**, in order to perform customs formalities. The complexity and continuous development of the customs legislation is forcing companies to turn to outside professionals. This option may be more cost effective than in-house operations for reasons of economic scale, expertise, technology, and the stimulation provided by competition in the private sector.

**International freight forwarders**, in order to perform customs and logistic formalities. A freight forwarder does not move the goods but acts as an expert in the logistic network. A freight forwarder contracts with carriers to move the goods and has additional experience in preparing and processing customs and other documentation and performing activities pertaining to international shipments.

Special attention is drawn to the fact that in case strategic services are outsourced to contracted persons, the applicant has to ensure that the knowledge and competencies required to deliver the service are constant during the contracted period. The person fulfilling the criterion and the applicant cannot be dissociated, as Article 38 paragraph 1 UCC stipulates that the criteria must be met by the economic operator who applies for the AEO status. The economic operator therefore has to be aware that it is possible to outsource “activities” but not the responsibility. As already stated above, low quality of service can eventually result in problems relating to the fulfilment of the other criteria, eventually resulting in suspension or revocation of the authorisation.

In this regard, where the applicant outsources the managing/handling of customs matters to a contracted person, the contract or any other type of agreement between the applicant and the contracted person must be made available to the customs authorities to clarify the capacity and responsibility of this contracted person and to consequently prove the compliance with the criterion.

## **Verification of the fulfilment:**

If the customs activities are outsourced to a third contracted party, the ICA has to check the fulfilment of the condition by:

- 1) Verifying if the applicant has a more than three years established relationship with the contracted person. To prove this the ICA can check the existence of a contract, mandate or any other type of agreement between the applicant and the contracted person that clearly states the operations and responsibilities the contracted person performs on behalf of the applicant (the contract or mandate are the copies held by the applicant) or
- 2) in case the established relationship is less than three years, verifying if the contracted person has an authorisation for customs simplifications where applicable, and/or has carried out customs formalities at least for three years.

As provided by Article 27 (2) UCC IA, the condition of "practical standards of competence" shall be considered fulfilled if the contracted person is an AEOC.

In case of outsourced customs activities it is sufficient that either the applicant, the applicant's employee in charge of customs matters or contracted person fulfils the criterion. If the applicant outsources its customs activities to more than one contracted person, the criterion must be fulfilled by all of them.

It should be noted that in case the applicant has an internal office or department involved in customs matters which allows the supervision and control on the customs formalities that have been outsourced, the criterion can be fulfilled by the applicant.

### **2.IV.2.2. A quality standard concerning customs matters adopted by a European Standardisation body**

It is to be noted that the competent European Standardisation Body has not yet developed standards applicable to "customs matters".

### **2.IV.3. Professional qualifications**

#### **Scope**

According to Article 27 (1) (b) UCC IA the criterion shall also be considered to be fulfilled if the applicant or the person in charge of the applicant's customs matters has successfully completed training covering customs legislation consistent with and relevant to the extent of his or her involvement in customs related activities, provided by any of the following:

- (i) *a customs authority of a Member State;*
- (ii) *an educational establishment recognised, for the purposes of providing such qualification, by the customs authorities or a body of a Member State responsible for professional training;*
- (iii) *a professional or trade association recognised by the customs authorities of a Member State or accredited in the Union, for the purposes of providing such qualification.*

## **Verification of the fulfilment**

Public or private institutions such as universities, customs schools, other specific schools or professional or trade associations that provide different courses to prepare for the recognition of a specific professional authorisation/accreditation/register for specific economic operators (e.g. the profession of customs agent).

The training body has to certify the successful completion of the course by the trainee.

The applicant or the persons in charge of the applicant's customs matters who are authorised or certified or have a license for the exercise of the professional activity related to customs matters (e.g. customs agents or freight forwarders) can demonstrate the respective proof to meet the criterion of a successful completion of a training covering customs matters.

It is also possible that a person inside the company, who has the legal power to physically represent the company, has successfully passed training in customs matters (e.g. a person in charge of the applicant company providing brokerage services such as the president or a member of the board, has successfully passed an exam as customs agent). In this case the applicant fulfils the condition of professional qualification through this person.

Besides it is further possible that Member States do not have any accreditation programmes or professional register, but have specific training in customs matters (e.g. education offered at a secondary school level or conventions with public bodies providing educational services). This type of training should be recognised by the customs authorities as sufficient in a specific professional context. Member States are encouraged to further develop such training schemes.

Customs authorities or public or private sectors listed in points ii) and iii) above, wishing to implement training for the fulfilment of the condition of professional qualification could consider the EU Customs Competency Framework for the Private Sector published on the TAXUD website:

[http://ec.europa.eu/taxation\\_customs/common/eu\\_training/competency/index\\_en.htm](http://ec.europa.eu/taxation_customs/common/eu_training/competency/index_en.htm)

This tool is underpinned by a set of core values which should be demonstrated by any trader or any individual working within the private sector and interacting with customs administrations of the EU.

## **Section V - Appropriate security and safety standards**

### **2.V.1. General**

According to Article 39 (e) UCC an AEO authorised for security and safety has to meet appropriate security and safety standards, which shall be considered as fulfilled where the applicant demonstrates that he or she maintains appropriate measures to ensure the security and safety of the international supply chain including in the areas of physical integrity and access controls, logistical processes and handling of specific types of goods, personnel and identification of his or her business partners. Article 28 UCC IA further elaborates the requirements to be met. It has to be clearly indicated, that the criterion of security and safety is only relevant if an economic operator applies for an AEOS.

At the same time it is important to know that examinations of the security and safety criterion shall be carried out for all the premises which are relevant to the customs related activities of the applicant. For example, a warehouse where goods, which are not under customs supervision, but which are intended to be exported (and so to enter an international supply chain), are stored has to be secured. On the contrary, a warehouse where only goods in free circulation are stored that will be sold inside the Union customs territory might not be relevant for security purposes. Thus, while preparing their application, operators must be able to identify activities in all their premises.

Only in case of a large number of premises, where the period for issuing the authorisation would not allow for examination of all the relevant premises, but the customs authority has no doubt that the applicant maintains corporate security standards which are commonly used in all its premises, the ICA may decide to only examine a representative proportion of those premises. This decision can also be reviewed during the monitoring process. Thus, premises not visited before can be included in the monitoring plan.

As each company is structurally different from another and has its own business model, the security and safety measures implemented by the applicants have to be considered on a case by case basis by the customs authorities. The aim of this section is not to provide an exhaustive list of all the security and safety measures that applicants could implement to comply with AEO security and safety requirements, but to rather give guidance to understand the concept of AEO security and safety. Examples of possible solutions of measures to be taken can be found in the [SAQ explanatory notes](#) and the relevant section of [Annex 2 of these Guidelines](#).

The applicant's security and safety standards shall be considered to be appropriate only in case all the conditions listed in Article 28 (1) UCC IA can be verified by customs authorities and deemed to be fulfilled. However, for the purpose of establishing compliance with Article 28 (1) (a) to (c) UCC IA minor shortcomings under one condition may be overcome by strengths under another condition. The meaning and the aim of the provision should always be kept in mind, namely that there are appropriate control measures in place to reduce the level of risk to an acceptable level. For example, there may be shortcomings in the background checks that are carried out on temporary staff. However the applicant recognises and effectively manages this risk by putting in place appropriate access controls to ensure that those temporary staff do not have unsupervised access to goods in/entering the supply chain or to security sensitive areas of the business. In that light it should also be reflected that good awareness and practical application of the AEO concept by the applicant and its employees may avert a minor risk due to lack of physical controls. On the other hand the best physical security and safety measures may fail without the necessary awareness of the competent staff.

While some of the criteria presented in [Part 2 'AEO criteria' of these Guidelines](#) may be checked on the basis of either documentation presented or on the spot, the security and safety criterion always has to include physical checks at the premises of the applicant.

Consideration should be given to a stepped approach depending on the risk of different areas (onion peeling principle).

Due account has to be taken to the provisions of Article 28 (2) and (3) UCC IA:

- *Where the applicant is a holder of a security and safety certificate issued on the basis of an international convention or of an International Standard of the International Organisation for Standardisation, or of a European Standard of a European standardisation body, these certificates shall be taken into account when checking compliance with the criteria laid down in Article 39(e) of the Code.*

*The criteria shall be deemed to be met to the extent that it is established that the criteria for issuing that certificate are identical or equivalent to those laid down in Article 39(e) of the Code.*

*The criteria shall be deemed to be met where the applicant is the holder of a security and safety certificate issued by a third country with which the Union has concluded an agreement which provides for the recognition of that certificate.*

Detailed information on Mutual Recognition and its implementation is included in [Part 6 of these Guidelines](#).

- *Where the applicant is a regulated agent or a known consignor as defined in Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council<sup>10</sup> and fulfils the requirements laid down in Commission Implementing Regulation (EU) 2015/1998<sup>11</sup>, the criteria laid down in paragraph 1 shall be deemed to be met in relation to the sites and the operations for which the applicant obtained the status of regulated agent or known consignor to the extent that the criteria for issuing the regulated agent or known consignor status are identical or equivalent to those laid down in Article 39(e) of the Code.*

## **2.V.2. Building security**

To prevent tampering with goods but also to protect sensitive data and documentations the applicant shall ensure that “*buildings to be used in connection with the operations relating to the AEOS authorisation provide protection against unlawful intrusion and are constructed of materials which resist unlawful entry*”.

The aim of security measures to secure buildings is to prevent unlawful intrusions and in case of intrusion of the perimeter fence/building allowing for:

- delay and deter the intruder (i.e. grids, codes, external and internal windows, gates and fences secured with locking devices);
- fast detection of the intrusion (i.e. access monitoring or control measures such as internal/external anti-burglar alarm systems or CCTV (close circuit TV systems);
- fast reaction to the intrusion (i.e. remote transmission system to a manager or to a security company in case alarm goes off).

---

<sup>10</sup> Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

<sup>11</sup> Commission Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security

This condition has always to be reflected in the context of access controls and cargo security. Indeed, security measures need to be reflected as a whole: if applicants want to protect their property (goods, data, buildings), they cannot strictly separate building security and access controls from cargo security measures.

Moreover, for risk analysis purposes, applicants as well as customs authorities shall take into account particular characteristics of each location. In some cases a premise will only consist of a building which therefore serves at the same time as an external boundary for the premises of the company; in other cases a premise will be situated in a well secured and controlled area such as a freeport, industrial zone, logistics park etc. In some cases even the loading ramp for incoming or outgoing goods will be part of the outer shell.

Even the premises layout (e.g. a surrounding with a high criminality or a greenfield development site, near or attached to other buildings, close to roads or railroad tracks) may influence the necessary measures to be taken. The premises layout may also influence the assessment of criteria Article 28 (1) (a) UCC IA “building security” and (b) “access controls”. Aspects to be taken into account when assessing this condition may, for example, be that a fence is set up at the ridge of a slope or on an embankment which elevates it or bordered by a hedge or a watercourse that make access to the building difficult.

While checking this condition it is of great importance to take due account that each applicant has to ensure the security of its buildings and access control, however when assessing the way it is achieved the specific characteristics of **SMEs** shall be taken into account. For example, a large manufacturer might have to have a perimeter wall/fence, security guards and CCTV (close circuit TV systems) etc. while for a customs agent operating from very limited premises, it might be sufficient to have in place proper secure locks on doors, windows and filing cabinets.

### **2.V.3. Appropriate access controls**

To secure the access to the premises and to prevent tampering with goods the applicant shall have “*appropriate measures in place to prevent unauthorised access to offices, shipping areas, loading docks, cargo areas and other relevant places*”.

There may be cases in which exterior security measures like fences, gates and lighting will be mandatory (when goods are stored outside of buildings, when the buildings walls are not regarded as an external perimeter or when all the buildings’ protection and access are not secured enough). On the other hand there may be cases where a complete exterior circular wall will not be possible and necessary. This might be the case if the applicant leases parts of an industrial or logistic park, no goods are stored outside and the other physical security requirements like building security are of high standard.

All security sensitive areas must be protected against unauthorised access from third parties but also the applicant’s own personnel who have no competence or appropriate security clearance to access those areas. This includes not only access control of unauthorised persons, but also of unauthorised vehicles and goods.

There should be routines in place and duly implemented on how to respond to security incidents in the case of an unauthorised access or attempt to access the premise (e.g. contact local police, internal security staff and as the case may be customs authorities). In this context

it is also important to know that the AEO security concept aims at prevention of incidences. Therefore, it is necessary to indicate any security breaches in advance before they can have an impact on the security and safety of the international supply chain in an essential way. An example may be a CCTV-system which only records, but is not monitored. While it may be sufficient for other purposes, it may not be sufficient for AEOS.

While checking this condition, it is of great importance to take due account of the specific characteristics of **SMEs**. Even though SMEs have to comply with the same requirements as a Large Scale Enterprise (LSE) with regard to the internal control procedures for access, different solution may be suitable for them concerning access controls. For example:

- most of the time, small businesses and micro-enterprises do not have enough resources to dedicate employees to monitor the access to the site. In this case, for example, an enclosed fence equipped with an intercom should allow access remote control to the site;
- an instruction recalling the obligation to maintain the shipping areas' doors lock closed and that the doors must be equipped with a bell for the drivers who want to access the shipping area, could prevent unauthorised access to cargo areas;
- while large companies are expected to issue identification tags to all staff and visitors, this might not be necessary in case of SMEs.

#### **2.V.4. Cargo security**

To ensure the integrity of cargo and to prevent irregular practices in the flow of goods within the international supply chain, the applicant shall have established “*measures for the handling of goods which include protection against the unauthorised introduction or exchange or mishandling of goods and against tampering with cargo units*”.

These measures, where appropriate to the business concerned, shall contain:

- integrity of cargo units (including usage of seals and 7-points inspection (outside, inside/outside doors, right and left side, front wall, ceiling/roof, floor/inside));
- logistical processes (including choice of freight forwarder and means of transport);
- incoming goods (including checking of quality and quantity, seals, where appropriate);
- storage of goods (including stock-checks);
- production of goods (including quality inspections);
- packing of goods (including the information on the packaging);
- loading of goods (including checking quality and quantity and sealing/markings).

Where appropriate and feasible, the above measures shall be documented and recorded.

Again, breaches of the integrity of the cargo/cargo units should be recognised at the earliest possible stage, reported to a designated security department or staff, investigated and recorded in order to take necessary countermeasures. Thus, it is also essential that competences and responsibilities between involved units and parties are clearly described and known.

As already mentioned under [2.V.2. of these Guidelines](#), cargo security is inseparable from building security and access controls as the ultimate aim of security and safety measures is to secure goods by preventing in particular unauthorised access to cargo (shipping areas, loading docks and cargo areas).



Moreover, while checking this condition it is of great importance to take due account of the specific characteristics of SMEs. For example:

- closed doors/railings, propitiatory sign and instructions may be sufficient to restrict access to authorised personnel only to restricted areas (these instructions may be incorporated into the general security and safety procedures of the applicant);
- to prevent unauthorised access in manufacturing areas, shipping areas, loading bays, cargo areas and offices, visitors could be escorted systematically in the premises and sign a register at the entrance.

Finally, cargo security is also inseparable from “Business Partner Security” because when goods in cargo units enter the supply chain, they are often placed under business partner responsibility.

## **2.V.5. Business Partner Security**

### **2.V.5.1. General**

**Business partner** is a term used to describe a commercial entity with which another commercial entity has some form of business relationship to the mutual benefit of both. For AEO purposes, relevant are business partners with direct involvement in the international supply chain.

All economic operators in the international supply chain that fall between the exporter/manufacturer and the importer/buyer may be regarded as business partners to each other depending on the particular situation.

The relationship with business partners may be contractual where the rights and obligations of both parties are set out in a legal contract. Alternatively, it may be a very loose arrangement without legal basis or it may be somewhere between both of these extremes (where documentation exists but is simply a statement of fact or intention). There may also be relationships where one party, e.g. a government owning and operating transport infrastructure and facilities, essentially determines the service parameters that another party, e.g. a carrier, can either accept or not and has very little, if any, influence over these parameters.

The selection of business partners is of vital importance and applicants for AEO status should have a clear and verifiable process for selection of their business partners.

From an AEO perspective business partners as mentioned in Article 28 (1) (d) UCC IA may have the option to apply for the AEO status, but if they choose not to exercise that option or if established in a country where it is not possible to obtain an AEO status, they should provide adequate evidence to their AEO partner that they can meet an acceptable level of security and safety standards. The ideal scenario would of course be that a maximum number of participants in the international supply chain hold AEO status or equivalent to it granted by the competent authorities of any third country with whom the EU has concluded a MRA.

### **2.V.5.2. Identification of Business Partners**

When an international supply chain is being examined in the context of an AEO self-assessment, it is important that the role of every business partner is clearly identified. The role

of the business partner determines the level of risk involved, the level of security and safety awareness required from them and, alternatively the measures to be implemented by the AEO to mitigate the risks identified. The responsibilities of the AEO's business partners could be e.g. the following:

- **manufacturers and warehouse-keepers** should ensure and promote the awareness that premises should meet an acceptable security standard that prevents goods in production and/or storage from being tampered with, and prevent unauthorised access;
- **importers/freight-forwarders/exporters/customs agents** should ensure third-party agents have awareness of relevant border procedures and systems, and are familiar with the required documentation that needs to accompany goods in transit and for customs clearance;
- **carriers** should arrange that the transportation of goods is not unnecessarily interrupted, and that the integrity of the goods while in their custody is maintained and protected against unauthorised interference.

### **2.V.5.3. Security requirements for business partners**

Article 28 (1) (d) UCC IA stipulates that security and safety standards in relation to business partners shall be considered to be appropriate if *“the applicant has taken measures allowing to clearly identify his business partners and to ensure, through implementation of appropriate contractual arrangements or other appropriate measures in accordance with the applicant's business model, that those business partners ensure the security of their part of the international supply chain.”*

An AEO is primarily responsible for its part of the supply chain, for the goods which are in its custody, and for the facilities it operates. When granted, the AEO status only relates to the person that applied for it. However, the AEO is also dependent on the security standards of its business partners in order to ensure the security of the goods in their custody. It is essential that an applicant is aware of all roles in its business partners' supply chain(s) and that he or she makes any possible effort to ensure that its business partner are complying with the security AEO requirements.

It is expected that any applicant will ensure that his or her business partners are aware of their security and safety obligations and requirements and endeavour, where appropriate and feasible depending on their business model, to have written contractual agreements or other appropriate measures in place. The applicant should therefore, if necessary, when entering into contractual arrangements with a business partner, make any possible effort to ensure that the other contracting party assesses and enhances their supply chain security and includes details as to how this is to be achieved and provide evidence of it. Management of risk related to business partners is also essential. Therefore, the applicant should retain documentation in support of this aspect to demonstrate its efforts to ensure that its business partners are meeting these requirements or, alternatively, have taken mitigating actions to address any identified risks.

The applicant needs to be aware of who its new potential business partners are. Also the AEO, once the authorisation has been issued, when considering new potential business partners,

should endeavour to obtain information about those aspects of the potential new partners' business which are of relevance to the AEO status.

Examples of how an AEO, or the applicant, could enhance its supply chain security are:

- works together with other AEO's or equivalent;
- enters, where appropriate and feasible according to its business model, into contractual arrangements on security with its business partners;
- subcontractors (for example transporters, hauliers, etc.) are chosen on the basis of their adherence to certain security rules and sometimes applicable mandatory international requirements in particular if they have been already approved under other security schemes such as KC or RA;
- contracts contain clauses preventing the subcontractor from further subcontracting the work to parties unknown for which the procedure in place for identification and to ensure appropriate security measures cannot be proved by the subcontractor. This should always be the case where secure air cargo/air mail is being transported from a known consignor;
- seals should be used for all modalities whenever possible to detect intrusion through the entry point(s) into the cargo compartment. Loaded containers should be sealed, by the party stuffing the container immediately upon completion of the stuffing process, with an ISO17712 compliant seal;
- loaded containers are inspected at the subcontractor's premises, the terminal and recipient premises to verify that they have been sealed;
- 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 applicant/AEO carries out or requires third party security audits of the business partner to ensure they comply with their security obligations and requirements;
- the applicant/AEO, where appropriate and feasible considering its business model, asks for a security declaration reflecting parties' respective business models, roles and responsibilities.

An example of security declaration that can be used in Member States is attached in [Annex 3 to these Guidelines](#) in cases where the applicant wishes to meet the requirements set out in Article 28 (1) (d) UCC IA by means of a security declaration from a particular business partner. However, in case the use of a security declaration is chosen as being an appropriate and feasible mechanism considering its business model, the applicant should be in a position to ensure that the obligations covered by it are really in place and observed by the relevant business partner.

- the applicant / AEO uses carriers, hauliers and/or facilities that are regulated by international or European security certificates (for example ISPS Code and RA).
- the applicant / AEO enters into non-contractual arrangements to specifically identify issues of importance relating to security, especially where potential weaknesses have been identified in a security assessment.

Both customs authorities and economic operators should take into account that the above mentioned measures are only examples and this list is not exhaustive. The choice of one or another measure or combination of measures depends very much on the role of the particular business partner in the supply chain and the associated risks and its business model.

Regardless of what measures the applicant has taken to comply with this requirement, it is important that procedures are in place for the monitoring of the arrangements with business partners and these are reviewed and updated on a regular basis.

If an applicant/AEO has information that one of its business partners, who is part of the international supply chain, is not meeting established appropriate security and safety standards, it shall immediately take appropriate measures to enhance supply chain security, to the best of its ability.

Regarding consignments taken over from unknown trading partners it is recommended that the applicant/AEO takes appropriate measures to mitigate the security risks related to that particular transaction to an acceptable level.

For example where air cargo/air mail arrives from an unknown trading partner for which the procedure in place for identification and appropriate security measures cannot be proved, it should be screened by a regulated agent.

This is particularly relevant where the applicant/AEO has new or temporary business partners or is involved in the transport of high volume consignments such as in the postal and express courier businesses.

In case of multiple subcontracting, the responsibility for securing the supply chain is transferred from the applicant/AEO (e.g. an exporter) to its own business partner (e.g. a freight forwarder). Indeed, this business partner is the one who has formally committed to secure the respective tasks on behalf of the applicant/AEO. However, if the “first degree subcontractor” (e.g. the freight forwarder) further uses other parties he or she should check the implementation of the security measures by the next subcontractor(s) (e.g. the carrier, or other subsequent freight forwarder).

If the AEO discovers compliance difficulties, it should contact the customs authorities with details of such occurrences without any delay.

#### **2.V.6. Personnel security**

Personnel security is along with the physical security, access controls, security of business partners etc. one of the main aspects of security. It is to be noted that this condition is not related to the "safety at work" as this is out of the scope of safety and security criterion

To prevent infiltration of unauthorised staff that could compose a security risk, the applicant shall “conducts, in so far as national law permits, security screening on prospective employees working in security sensitive positions and carries out background checks of current employees in such positions periodically and where warranted by circumstances”.

With regard to the practical implementation of this requirement the following important issues have to be taken into account both by the customs authorities and by the applicant:

- all economic operators should have in place appropriate system/procedures to comply with this requirement and customs authorities have to be able to verify this;

- it is the applicant, being the employer, who is responsible for conducting these checks while customs authorities verify whether they are done and whether they are sufficient to ensure compliance taking into account prevailing legislation;
- scope and purpose of the checks should be clear. The proportionality principle should be respected i.e. ‘action should not go beyond what is necessary with regard to the purpose’.

The extent and evaluation of the condition fulfilment depends on the size, organisational structure and type of the business activity of the economic operator. Therefore, a particular verification is adjusted to the applicant concerned. However, the main areas that should be always checked include:

*- employment policy of the applicant*

The general organisation and procedures for the recruitment of new staff have to be clear including who is responsible for it. The applicant’s policy should particularly reflect all reasonable precautions to be taken into account when recruiting new staff to work in security sensitive positions to verify that they are not previously convicted of security-related, customs or other criminal offences related to the security of the international supply chain, and conduct periodic background checks for established staff in security sensitive positions with the same intent both to the extent permitted by national legislation.

Security checks methods may comprise basic checks like verifying the identity and the residence, checking the labour permit if necessary before recruitment, conducting a self-declaration of criminal records and inquiries based on undeniable and/or official elements of previous employment history and references.

The applicant should also have security requirements in place regarding the use of temporary personnel and agency workers. Similar security standards for temporary and permanent staff as well as agency workers are required taking into account the security sensitiveness of the positions. If an employment agency is used to recruit personnel, the applicant should specify, in contracts with the agency, the level of security checks to be performed on staff prior to and after recruitment to security sensitive positions. Customs auditors may ask to verify how the applicant's checks on external staff are carried out. In this respect, the applicant should maintain evidences of the applied standards within its records.

*- employees working in security sensitive positions*

When defining the ‘security sensitive positions’ appropriate risk analysis should be done and it has to be taken into account that these are not only management positions, but also positions related directly with the handling, storage and movement of goods. Security sensitive positions in this context are for example:

- positions with responsibility for security, customs or recruitment matters;
- jobs assigned to the buildings and reception supervision;
- workplaces described in [Section 6 of the SAQ](#) related to incoming/outgoing goods and storage.

These checks may also concern existing employees coming from other departments, not regarded as sensitive from a security point of view, and moving to such posts.

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.

It should also be recommended that the employed personnel are not listed in one of the blacklists which are established by national or supranational law (e.g. Regulation (EEC) No 2580/2001<sup>12</sup>, Regulation (EEC) No 881/2002<sup>13</sup> and Regulation (EU) No 753/2011<sup>14</sup>).

Any checks to be done have to be in conformity with any EU and/or national law on personal data protection that regulates the processing of personal data under different conditions. In a number of cases there are provisions that allow treatment of personal data only in case the person concerned has given his or her consent for this in advance. Thus, in order to facilitate the process for some of the positions, a special clause may be included in the contract that asks the person concerned to give his or her consent for doing the so called background checks.

*- policy and procedures when staff leaves or are dismissed*

The applicant should have procedures in place to expeditiously remove identification, premises and information systems access for employees whose employment has been terminated.

As mentioned in the [SAQ explanatory notes](#) (see question 6.11 “*Personnel security*”), all of these security requirements implemented with regard to the applicant’s employment policy should be documented.

## **2.V.7. External service providers**

The applicant may also have contractual business relationships with other parties including cleaners, caterers, software providers, external security companies or short-term contractors. For AEO purposes, these parties are referred to as service providers.

Article 28 (1) (f) UCC IA requires that *"the applicant has appropriate security procedures in place for any external service providers contracted"*.

Although external service providers do not have a direct role in the international supply chain, they may have a critical impact on the security and customs systems of the applicant. Therefore, in terms of security and safety the applicant should apply appropriate measures to them just as he or she should for his or her business partners.

Where some of the AEO security and safety conditions are fulfilled by the service provider on behalf of an AEO applicant, this will need to be verified as part of the audit. A typical

---

<sup>12</sup> COUNCIL REGULATION (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism

<sup>13</sup> COUNCIL REGULATION (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated

<sup>14</sup> COUNCIL REGULATION (EU) No 753/2011 of 1 August 2011 concerning restrictive measures directed against certain individuals, groups, undertakings and entities in view of the situation in Afghanistan

example is the condition for access control when the applicant has contracted a security company to fulfil its obligations in this area. The access control condition has to be verified by assessing the way the service provider fulfils this on behalf of the AEO. Although the AEO may outsource these activities to a third party, it is the AEO who, because the service partners acts on its behalf is and remains responsible for compliance with the AEO criterion and ensuring the service provider complies with the requirements.

## **2.V.8. Security awareness programmes**

To prevent inadequate awareness of security requirements the applicant shall “*ensure that its staff having responsibilities relevant for security issues regularly participates in programmes to raise their awareness of those security issues*”. The applicant should develop mechanisms in order to educate and train staff on security policies, recognition of deviations from those policies and understanding what actions should be taken in response to security lapses.

The applicant should particularly:

- educate its personnel, and where appropriate its business partners, with regard to the risks in the international supply chain;
- provide educational material, expert guidance and appropriate training on the identification of potentially suspect cargo to all relevant personnel involved in the supply chain, such as, security personnel, cargo-handling and cargo-documentation personnel, as well as employees in the shipping and receiving areas. This training should be in place before the economic operator applies for the AEO status;
- keep adequate records of educational methods, guidance provided and training undertaken to document the awareness programmes;
- provide for a service or a person (internal or external to the company) responsible for the training of personnel;
- make employees aware of the procedures which are in place within the company to identify and report suspicious incidents;
- conduct specific training to assist employees in maintaining cargo integrity, recognising potential internal threats to security and protecting access controls;
- revise and update the content of training regularly when readjustments are necessary. The content of the training should reflect any specific requirement related to the specific business activity of the economic operator, e.g. air cargo/air mail.

There is no mandatory frequency in which safety and security training should be repeated. However, as staff, buildings, procedures and flows can change frequently, awareness levels need to be maintained by ensuring training is refreshed and updated on a regular basis.

Moreover adequate training is mandatory for all new employees or for any employee of the company newly assigned to a post in connection with the international supply chain.

The above listed mechanisms for the education and training of personnel regarding security policies should be, of course, appropriate to the size of the enterprise (See Part 3, Section III, point 3.III.2. 'Small and medium sized-enterprises'). For example, for micro **SMEs**, an oral training, however documented, and a recall of basic security and safety requirements in the general security and safety procedures or a simple note of awareness, initialled by the staff concerned may be accepted by customs authorities.

At the same time the frequency and the intensity of the security and safety training may vary between different employees in one enterprise due to their responsibility and their individual possibility to influence the security of the international supply chain.

Applicants and their employees are encouraged to use the Commission AEO eLearning tool to gain a general understanding of the AEO concept and the related security requirements.

#### **2.V.9. Appointed contact person**

Article 28 (1) (h) UCC IA foresees that *"the applicant has appointed a contact person competent for safety and security related questions"*. This contact person has to be nominated to the ICA. It is to be noted that this condition is not related to the "safety at work" as this is out of the scope of safety and security criterion

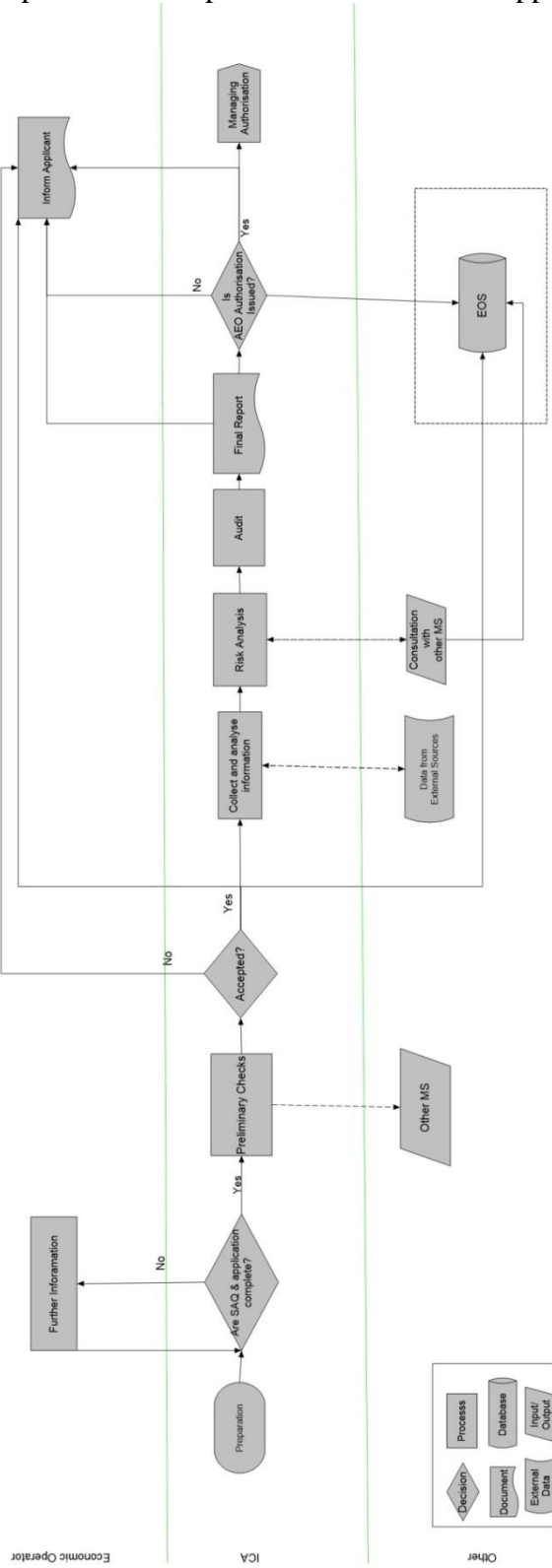
This person should be the contact point for any issues originating from inside the company and also those originating from the ICA relating to safety and security.

Whether this function is outsourced or not, it is to be ensured by the applicant that this person is fully aware of all specific security related issues of the company and is authorised to receive and communicate security sensitive material.



### PART 3, Application and authorisation process

The following flowchart provides a simplified overview of the application process:



## **Section I - Determination of the competent Member State for submitting an AEO application**

### **3.I.1. General:**

The Member State to which the AEO application should be submitted is determined in the third sub-paragraph of Article 22 (1) UCC. This states that the competent customs authority shall be that of the place where the applicant's main accounts for customs purposes are held or accessible, and where at least part of the activities to be covered by the decision are carried out. The general principle is that the application should be submitted to the Member State which has the best knowledge of the applicant's customs related activities.

Nevertheless, considering the modern trends in companies' organisational structures and business flows, as well as of the ongoing trend on outsourcing certain activities, the correct decision is not always "at hand".

Whenever it is not possible to determine clearly the Member State which should act as ICA based on the above mentioned general principle, Articles 12 or 27 UCC DA apply.

Article 12 UCC DA establishes that the competent customs authority shall be that of the place where the applicant's record and documentation enabling the customs authority to take a decision (main accounts for customs purposes) are held or accessible (e.g. the place where the administrative headquarter of the applicant company is located).

Article 27 UCC DA, specifically for AEO, states that where the competent customs authority cannot be determined in accordance with the third subparagraph of Article 22 (1) UCC or Article 12 UCC DA, the application shall be submitted to the customs authorities of the Member State where the applicant has a permanent business establishment and where the information about its general logistical management activities in the Union is kept or is accessible as indicated in the application.

### **3.I.2. Accessibility of customs related documentation**

The third subparagraph of Article 22 (1) UCC is also addressing the situation where a company is outsourcing its customs related administration to an entity in another Member State or in a third country. This practise is usual and legally allowed in many Member State. In these cases, the company ensures that the customs authority of the Member State where it is established has electronic access to the documentation held in another Member State or in a third country.

In these cases, the application has to be submitted in the Member State to which the company ensures the accessibility to the main accounts and at least part of the customs related activities are carried out.

Example 1:

Company "C" is established in SE. It carries out all its business activities in SE, except that the administration is outsourced into EE. It ensures electronic access to its documentation to the Swedish customs authorities as defined by the relevant rules in SE:

*The AEO application is to be submitted in SE.*

A different situation is where customs activities are not carried out in any of the Member State where documentation is kept or accessible.

Example 2:

Company "C" is established in the UK. It outsources its records and documentation enabling the customs authority to take a decision (main accounts for customs purposes) to IE and they are accessible from the UK. It imports goods from Asia through RO:

In this case Article 12 UCC DA applies and *the AEO application is to be submitted in the UK.*

Example 3:

Company "C" is established in IT. It has its main accounts in MT, not accessible from anywhere else. It imports from UA. Imports and storage takes place in DE. Manufacturing takes place in ES. Exports take place from PT.

In this case the application is to be submitted in MT as the main accounts are only accessible here.

### **3.I.3. Multinational companies and large businesses**

As explained above, it is clear that any economic operator who is an autonomous legal entity has to submit its own application together with a thoroughly filled [SAQ](#). Multinational companies do in some cases operate through separate legal entities in different Member States, while in other cases they operate through PBEs.

According to Article 5 (32) UCC a PBE is defined as "*a fixed place of business, where both the necessary human and technical resources are permanently present and through which a person's customs-related operations are wholly or partly carried out*". It is to be noted that in line with Article 5 (31) (b) UCC a PBE is not an autonomous legal entity. Nevertheless, the legal status of PBEs can be defined differently according to national legislation. In fact, PBEs, in order to operate, in some Member States may be considered as autonomous legal entities even if the corporate group they form part of considers them as non-independent from an internal point of view. In this case the general principle stated above applies: that is, the "PBE" has to apply separately.

Example 1:

A parent company "P" is established in DE. It has the following legal independent PBEs: "PBE1" registered in BE and "PBE2" registered in AT. The parent company "P" is not carrying out any customs related activities, but its PBEs are involved in activities covered by customs legislation. Parent company "P" would like to get the AEO status for the whole group. The main accounts related to customs activities involved as well as the customs related activities are performed in the Member States where the PBEs are registered:

*"PBE1" has to submit an application in BE, and "PBE2" has to submit its own application in AT, whereas parent company "P" which is not involved in customs related activities is not qualified to apply.*

It is to be noted that indeed separate applications are to be submitted and this would seem to be a burden for the applicant. Nevertheless, it is worth considering that the two applications are completely separate and as a result non-compliance with some criteria for one application would not result in rejecting the application for the other PBE or, if the authorisation has already been issued, to its suspension or revocation.

In the cases where PBEs are not independent legal entities, according to Article 26 UCC DA one single application has to cover “all its (the applicants) PBEs in the customs territory of the Union”. Article 27 UCC DA provides that in the cases of single application as referred to in [Part 1, Section II, point 1.II.1. of these Guidelines](#), the application shall be submitted to the customs authorities of the Member State where the applicant has PBEs and where the information about its general logistical management activities in the Union is kept or is accessible as indicated in the application.

**Example 2:**

A parent company 'A' is established in the UK. It has PBEs which are not separate legal persons in BE, DE and the NL; the information related to its general logistic management is in the UK:

*Only one single application has to be submitted by company 'A' including all branches. In the [SAQ](#) common procedures as well as branch typical processes have to be described.*

The situation is similar for a third country company having PBEs in the Union.

**Example 3:**

A parent company 'A' is established in the US. It has PBEs which are not separate legal persons in the UK, BE, DE and the NL. The PBE in the UK has the role of a European centre and as such information related to its management system for the activities in all the branches in the EU are held in the UK. Customs related activities are done in the UK, BE, DE and the NL:

*Only one application has to be submitted by company 'A' in the UK. However, the following information has to be included in the application:*

- Box 1 = name of the parent company in the UK and the names of the branches in BE, DE and the NL;

Box 4 = addresses of the branches in BE, DE and the NL;

Box 9 = the EORI number of the company in the UK and the relevant registration numbers (VAT or TIN if VAT is not available) of the branches in BE, DE and the NL

Box 16-18 = offices of all EU branches.

Member States are encouraged to consult each other at an early stage, even before accepting the application of such a third country applicant, in order to clarify that all PBEs of the applicant in the territory of the Union are included in the application.

To determine where to lodge the application in the above mentioned cases see [Part 3.I.2](#) above.

## Section II - Receipt and acceptance of the application

The general process to be followed when an application for an AEO status has been submitted is described in Articles 22 and 38 UCC, Articles 11 to 13 and 26 to 28 UCC DA and Articles 10 and 12 UCC IA. Until the date of the upgrading of the UCC AEO System the application shall be lodged using the information contained in Annex 1 C of the CCIP. Upon receipt of the application form, customs authorities examine it and decide upon its acceptance or non-acceptance. The following common general considerations have to be always taken into account:

- the application should be lodged according to the requirements of Article 22 (1) UCC, and Article 11 UCC DA
- a [Self-Assessment Questionnaire \(SAQ\)](#) shall be submitted with the application as provided by Article 26 (1) UCC DA
- customs authorities have to have all of the necessary information to be in a position to do the quick check of the application submitted against the conditions for acceptance. This can be sought by either accessing the relevant databases or asking the applicant to provide it together with the application;
- whenever appropriate, customs should also use other available sources of information e.g. common EU databases, contacts with other authorities, information from the company's web page etc.;
- in case additional information is required, customs authorities have to ask for it from the applicant as soon as possible but not later than 30 calendar days from the date of receipt of the application according to Article 22(2) UCC;
- where the customs authority establish that the application does not contain all the information required, it shall ask the applicant to provide the relevant information within reasonable time limit which shall not exceed 30 days according to Article 12 (2) 1<sup>st</sup> subparagraph UCC IA;
- customs authorities must always inform the applicant about the acceptance of the application and the date of acceptance; they should inform him also in case of non-acceptance of the application, stating the reasons for non-acceptance (second subparagraph of Article 22 (2) UCC);
- in the cases of applications received by multinational companies when taking the decision for acceptance/non-acceptance, please see also [Part 3, Section I 'Determination of the competent Member State for submitting an AEO application'](#) of these Guidelines.

As soon as the applicant receives the notification that his or her application has been accepted by Customs, it is strongly recommended that he or she does the utmost to speed up the overall process. In particular reviewing the following points throughout the whole application process is strongly recommended:

- *consolidation of the information and evidence of different units/departments related to the AEO application process;*
- *provision of information* - it is advisable that responsible units are aware of their specific responsibility regarding the overall AEO requirements/process and are ready to provide necessary information;

- *Follow-up* – the company should be taking actions to rectify weaknesses discovered during the filling up of the [SAQ](#) and mitigate the associated risks and customs should be informed about no compliance issues. It is also recommended to inform customs about the actions being taken;
- *Consultation of customs* – Clarify any doubt with customs the company may have, to avoid wasting time and money.

### **Section III - Risk analysis and Auditing process**

It is to be noted that the term customs audit covers different types of customs controls or assessments performed by customs to ensure that economic operators comply with Union and national legislation and requirements in customs related areas. Audit covers pre-audit, post clearance audit and re-assessment.

Pre-audit is performed by customs before the granting of any kind of customs authorisation/certification. In the context of AEO the pre-audit is the audit that follows the AEO application and serves to verify if the applicant fulfils the criteria laid down in Article 39 UCC. As a result of the (pre-)audit the auditor must be able to:

- make a judgement about the fulfilment of the conditions for the granting of the AEO status
- identify the remaining risks and propose further actions to be undertaken
- identify points in the operator's procedures which need a closer monitoring and advise the applicant to improve or strengthen the relevant procedures and controls.

Once the status is granted, one has to differentiate between monitoring and re-assessment. Monitoring is done continuously by customs authorities by supervising daily activities of the AEO including visits to his or her premises. It aims at the early detection of any signal of non-compliance and shall lead to prompt actions in case difficulties or non-compliance are detected. Re-assessment implies that something has already been detected and action has to be taken in order to verify if the economic operator is still compliant with the AEO criteria. In this context it is clear that monitoring can trigger re-assessment.

#### **3.III.1. Collect and analyse information**

In order to perform risk analysis and prepare an effective and efficient audit, it is vital for the ICA to get as much as possible and relevant information available about the economic operator. The information is collected with the purpose to:

- better understand the business of the economic operator and the environment of its activity;
- get the best possible overview of economic operators' business organisation, processes, and procedures;
- prepare the audit plan according to the risk evaluation results;
- prepare the audit (optimum audit team, focus of the audit, etc.);
- verify the fulfilment of the criteria as much as possible.

The information that can be obtained by customs authorities from various sources includes the following:

- internal databases (e.g. customs procedures used/declarations made by the applicant);

- internal information (result of previous checks and or audit; other authorisations granted or revoked and the supporting documents, review of previously submitted customs declarations, etc.);
- information requested from and provided by other authorities;
- information provided by other Member States (Information and consultation procedure – see [part 4](#) 'Exchange of information between Member States and with other government authorities' of these Guidelines);
- information provided by the economic operators themselves (i.e. [SAQ](#));
- publically available information (news, internet, studies, reports, etc.);
- any other relevant information including images, photos, video, premises' plan, etc.

All the information collected has to be carefully evaluated in order to assess its accuracy and relevance to the objectives of the auditing. It should be clear that collecting information is a dynamic process and it could well happen that “information asks for more information”. The applicant should be aware of this and be ready to provide customs with any additional information needed. Even once the examination has commenced, the auditors can ask and collect additional relevant information that adds value to the result. It should be also considered that information is changing and sometimes it is only valid at the time it is collected. Therefore, it is important to have the most recent and update information. To ensure that the ICA is up to date with events that can affect the outcome in the application phase and in the follow up work it is essential to have a system to capture and communicate to the applicant where more information is needed.

The size of the economic operator, its specificity, and cases where he or she has gone through other relevant accreditation processes could result in speeding up the process very much.

### **3.III.2. Small and medium-sized enterprises**

SMEs are defined in Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises<sup>15</sup>. This definition takes into account if an enterprise is part of a bigger multinational company, and in that case the enterprise cannot be considered as an SME.

For the purposes of the AEO authorisation and compliance with the requirements, it should be also taken into account that SMEs are all different in terms of size, complexity of the business, type of goods handled, position in the international supply chain etc. For example:

- an applicant with 51 employees importing glasses would be dealt with differently than an applicant with 249 employees importing weapons and who has already implemented various security measures;
- a customs agent with 4 employees acting as a subcontractor for another manufacturer with 150 employees also illustrates the variety of the SMEs' situation.

---

<sup>15</sup> Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises OJ L 124/2003

SMEs represent 99%<sup>16</sup> of all European businesses, and nine out of ten SMEs are actually micro enterprises with less than 10 employees.

They are also becoming an essential part of the international supply chains. In some cases, they may represent the bulk of economic operators in the international supply chains, often acting as subcontractors to larger companies.

Taking into consideration in particular the possible difficulty for SMEs in entering the authorisation process and in order to make the AEO status more available to SMEs, the necessary flexibility has been implemented in the AEO legislation to minimise costs and burdens. Even if the AEO criteria apply to all businesses regardless of their size, Article 29 (4) UCC IA 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, when examining the fulfilment of the AEO criteria"*. In parallel all along these Guidelines SMEs specificities regarding AEO authorisation will be treated through examples.

### **3.III.3. Specific economic activities**

#### **3.III.3.1. Express operator**

The role of a carrier in the international supply chain is described in [Part 1, Section II.4](#) paragraph (f) of these Guidelines. Within this trade sector there is a distinct sub-sector: express operators. This sub-sector involves a relatively small number of economic operators, but significant volumes of transactions; in some Member States this sub-sector accounts for about a third of all consignments at import and about 50% of all consignments at export.

This sub-sector has a number of distinct features:

- high volumes of transactions;
- the importance of speed of transport and fast clearance – quick delivery times are an important marketing tool for these businesses and important to their customers;
- a large number and range of business partners from regular business customers to one-off private customers;
- the economic operators often fulfil the role of customs agent/representative in addition to the role of carrier;
- as the mode of transport is mainly air freight these economic operators will operate as RA or KC as referred to in Regulation (EC) No 300/2008<sup>17</sup> and fulfil the requirements within Commission Implementing Regulation (EU) 2015/1998<sup>18</sup> for the majority of their business operations/activities;
- carrying packages and freight on their own aircraft or providing loaded bags and loose packages for other air carriers;

---

<sup>16</sup> In 2008, there were over 20 million enterprises in the European Union. Only about 43 000 were large scale enterprises (LSEs). Hence, the vast majority (99.8 %) of enterprises in the EU are SMEs. (*annual report – EU Small and medium enterprise 2009 - DG for Enterprise and industry*)

<sup>17</sup> Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002

<sup>18</sup> Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security



- the economic operators often hold authorisations from the customs authorities to use simplified customs procedures.

Given these distinct features there are a number of specific risks for this sub-sector that particularly need to be considered, when economic operators apply for the AEO status, i.e.:

- the level of infringements in assessing the customs compliance criterion. The customs authorities will need to take into account the high volume of transactions and assess whether infringements are systematic, the quality of the economic operators' internal controls and the procedures to identify and correct errors – see [Part 2 'AEO criteria' of these Guidelines](#);
- the security of data held in assessing the economic operator's system of managing commercial and, where appropriate, transport records. Given the high volume of data held, the customs authorities will need to consider the measures in place to protect the economic operator's systems against unauthorised access or intrusion and the access to documentation and the procedures for processing the information into the systems used by the express operators;
- In assessing appropriate security and safety standards:
  - o locations or activities that are not covered by the status of RA or KC;
  - o breaches of agreed security arrangements with the risk of delivering unsafe or unsecured goods. Given the wide range of business partners, the customs authorities will need to assess the procedures for selecting business partners and managing the risks associated with known and unknown trading partners;
  - o persons infiltrating the business that could pose a security risk. Given the high volumes of business the customs authorities will need to assess the procedures for performing background checks on new employees for both permanent and temporary personnel;
  - o inadequate awareness of security requirements. The customs authorities will need to assess the procedures for providing appropriate training covering the security and safety risks associated with the movement of express consignments.

### **3.III.3.2. Postal operators**

A postal operator has its own peculiarity and it is necessary to take in consideration its characteristics and the risks associated. As it can be assumed that the criterion on proven solvency shall be assessed in the same ways as for the others operators, the focus below will be on some specific issues related to the other AEO criteria.

#### **Customs Compliance**

A postal operator deals with delivery/dispatch service to a multiplicity of small clients/users whose reliability is not very easy to control. The consequences relates to possible problems with regard to customs duties, and also to security and safety compliance. Examples of risks areas related to customs operations could be the following:

- the high number of “small” shipments, i.e. low weight/value shipments;
- the unreliability of the statements made by the customers (mostly individuals): errors and omissions in the statements on the value and misdescription of the contents of shipments, lack/inadequacy of the supporting documents accompanying the customs declarations and the consequent difficulties in meeting customs requirements (lack of certifications/ licenses, etc.);

- delays in delivery caused by the carrier;
- high risk of "mishandled" (lost) shipments.

Therefore, during the auditing process for the customs compliance criterion, besides taking into consideration the size and type of the economic operator, the auditor should consider also the number of infringements compared to the total number of transactions lodged annually in order to evaluate the potential risks involved. The management of the procedure for the entry into the declarant's records with the waiver of the obligation for the goods to be presented and the customs warehousing procedure are the most important elements to be evaluated in a circumstantial way, evaluating also the remaining risks.

### **Accounting and logistic systems**

One of the risks to be taken into account is the management of inventories reporting undelivered mail/parcels (when it has not been possible to trace the recipient or when the recipient has failed to pick them up). Regarding this critical aspect, it is necessary to make an assessment of the costs of storage (and, if any, subsequent destruction, where specified by the rules) or the costs associated with the return to sender. This could heavily influence customs and accounting operations traceability and have an impact on the logistics organisation as well management, cost, stock safety and warehouse security.

Such an operational situation requires the possibility of relying on an IT system which has to be safe enough and structured in a way to ensure the audit traceability of all customs operations, both export and import, as well as the safety of the data contained therein.

When assessing the effectiveness of the internal control system, it is important to check, in addition to the segregation of duties, if there are people in charge of monitoring compliance with the rules regarding customs procedures and how the associated risks are actually detected and covered. Consequently, the impact of various possible negative events on the operator's activity should be assessed and the effectiveness of the procedures carried out to take action for resolving non-compliance should be carefully evaluated.

Besides, still in relation to internal control, it is important to check which databases and which information procedures are used for storing the data regarding customers and shipments.

Another aspect which should be evaluated is the management of land transport, especially if it concerns an airport operator, in which case it is necessary to assess the reliability of the drivers which retrieve packages.

### **Security requirements**

In this context the personnel recruitment should be carefully considered. It is important to consider the number of occasional workers and frequency with which they are engaged. The greater the number and the higher the frequency, the higher the potential risk of infiltration with the intention to perform illicit activities such as parcel bombs, drugs etc.

Therefore, the selection criteria adopted for recruiting the personnel to be assigned to special operations such as those in direct contact with sensitive goods from storage places or high risk areas, will have to be carefully evaluated.

It is necessary also to check the frequency with which the operator performs the monitoring of personnel as permitted by law. The contracts with the employees should also be carefully considered.

All staff, regardless of the type of contract under which they carry out their work, should be guaranteed adequate professional training, in particular regarding customs procedures and regulations. In order to achieve a high quality standard in the application of security and safety procedures, it is necessary to provide an adequate level of training including the staff dedicated to the scanning of particular goods to be shipped.

In order to ensure the security of the international supply chain, a postal operator should:

- draw up security and safety guidelines to inform and train staff on the risks related to postal operations;
- have an adequate internal organisation that allows increasing the frequency of inspections during specific risk events or following specific intelligence reports;
- train postal inspectors assigned to security checkpoints properly and provide them with an updated information on how to identify potentially dangerous shipments keeping into account risk indicators such as:
  - sender not indicated;
  - sensitive recipients (diplomatic, political institutions, financial bodies, religious communities, the press, etc.);
  - presence of markings or stickers aimed at avoiding controls like: "Do not expose to X-rays", "Confidential", "does not require post inspection ", "do not open" etc.;
  - unusual macroscopic physical and chemical characteristics (e.g. Hot Pack, presence of unusual odours, loss or spread of contents, packaging discoloration, oily spots, noises coming from inside, etc.).

A postal operator must also take measures for the logistic/organisational dimension of the spaces used for the storage of shipments through the following actions:

- have special areas where security controls of arriving or departing shipments can be carried out;
- physically separate the goods subject to control from those not yet inspected;
- require customers to use products which traceability can be assured;
- prepare a plan of reaction to identify, isolate and neutralise a detected threat;
- create a security contact office for customs, police, intelligence and health authorities according to the kind of service offered and its importance.

In conclusion, given the significant size and the special characteristics of the service offered by postal operators, as well as the number of transactions, and in order to put in place reliable procedures in terms of customs, logistics, accounting and security, it is essential that all procedures are strictly standardised, with detailed internal procedural protocols which are actually made operational in everyday practice.

### 3.III.3.3. Rail carriers

In general the audit of a rail carrier doesn't significantly differ from other carriers. It can be even considered that railway operators constitute a lower risk due to the nature of the transport mode. However, planning the auditing activities and assessing the risks will benefit from elaborating on a few distinct features in rail carriers' business operations:

- railroad operators are bound by **international agreements** and conventions (COTIF, CIM). These agreements may impose requirements related to seals and cargo integrity. Responsibility during transport might also be addressed;

- railroad traffic is subject to **rail safety regulations and certifications** concerning both passenger safety and cargo safety. These may include requirements of security management systems, personnel safety and internal control systems;
- rail carriers operate in a fragmented environment from a regulatory point of view. The railroad operations may be regulated and monitored by **several national authorities**;
- the operating environment contains several elements which are often controlled by third parties, responsible for the infrastructure such as tracks, marshalling yards and container terminals or third parties responsible for the cargo unit;
- the applicant might have a complicated organisational structure, a lot of premises and a wide range of operations. The operations can also be divided into passenger and cargo operations;
- rail carriers may operate with a multitude of business partners, regularly well-known. These may include for example road carriers, warehouse operators, harbour operators and service providers for security at railway yards. Loading and unloading of cargo units/containers from or onto a wagon can be in the responsibility of the carrier. However, loading and unloading of goods is regularly the customer's responsibility. Railway carriers regularly do not load or unload cargo units by themselves or by third parties. Only in case railway carriers offer parcel service and additional other logistic services by themselves, they may have the operational responsibility for the handling of the goods;
- during transport several persons might handle the documents or might control the cargo units/wagons. Only when railway carriers offer parcel service and additional other logistic services by themselves, they handle the goods in load transfer points, logistic centres or warehouses.

Points of attention during risk assessment and audit of a rail carrier applying for an AEO status:

- to better understand the business environment, the customs authorities should ask the applicant to give a short presentation on the regulations, agreements and conventions they are bound by before the audit;
- when preparing for audit, auditors should be able to establish a clear overview of sites and premises involved in customs operations and determine whether the applicant is in control of them or not. The relevant sites are premises where customs related documents, cargo units and goods are handled;
- preventing unauthorised access to goods and cargo units implies adequate security surveillance methods especially in open access railway yards and during transport/unloading/loading and halts;
- tracking of cargo units, security procedures related to border crossing (surveillance camera, scanning) and halts, weighing of cargo and 7 point inspection (especially after long-term storage);

- sealing procedures including instructions for security breaches;
- identification of business partners and incorporating security requirements into contracts, even for ad hoc partners. Due to outsourcing of key activities (loading/unloading/security surveillance) the applicant has to manage risks related to business partners through implementing requirements into contracts and monitoring them. Also routines when a security breach is noticed play an important role in enhancing the supply chain security;
- security awareness training is properly implemented;
- routines for informing about and handling security breaches are a key requirement.

### **3.III.4. Factors facilitating the authorisation process**

#### **3.III.4.1. General**

The different economic operators due to their economic activities have to fulfil different standards and regulations besides the AEO requirements. The AEO programme tries to consider and rely on already existing standards and certifications/authorisations, without including a requirement to have any additional certifications/authorisations to become an AEO.

While economic operators do not always need to have the AEO status in order to obtain an authorisation for a simplification provided for under the customs rules, for some simplifications they do need to fulfil certain AEO criteria or part of the AEO criteria to obtain the relevant authorisation (see also [1.III.1 of these Guidelines](#)).

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

- previous applications for customs authorisations and results of the process;
- information which has already been communicated to customs or other public authorities and that is available or accessible to customs;
- Information on and results of customs audits;
- customs procedures used/declarations made by the applicant;
- existing standards applicable to and certifications/authorisations held by the applicant;
- existing results of assessment or audit carried out in accordance with Union legislation to the extent they are relevant for the examination of the criteria (Article 29 (2) UCC IA) and existing conclusions of relevant experts (Article 29 (3) UCC IA).

However, depending on the circumstances of each individual case, taking mainly into consideration the time to which this information is related, customs authorities may need to re-examine or seek confirmation from other authorities in order to check that the information (wholly or in part) is still valid.

Specific attention shall be paid to the cases, where the legislation provides for automatic recognition of security and safety standards i.e.:

- Where the applicant is a regulated agent or a known consignor the safety and security criteria shall be deemed to be met in relation to the sites and the operations for which the applicant obtained the status of regulated agent or known consignor to the extent that the criteria for issuing the regulated agent or known consignor status are identical or equivalent to those laid down in Article 39(e) UCC (Article 28 (3) UCC IA, see also [Part 3, Section III, point 4.2.](#) (b) of these Guidelines);
- Where the applicant is a holder of a security and safety certificate issued on the basis of an international convention or of an International Standard of the International Organisation for Standardisation or of a European Standard of a European standardisation body, these certificates shall be taken into account when checking compliance with the safety and security criteria.  
The criteria shall be deemed to be met to the extent that it is established that the criteria for issuing that certificate are identical or equivalent to those laid down in Article 39(e) UCC (Article 28 (2) first subparagraph UCC IA).  
The criteria shall be deemed to be met where the applicant is the holder of a security and safety certificate issued by a third country with which the Union has concluded an agreement which provides for the recognition of that certificate (Article 28 (2) second subparagraph UCC IA).

This shall only be valid for certifications issued by internationally accredited certifiers<sup>19</sup> or national competent authorities.

Besides, there is a large number of international and national standards and certifications as well as conclusions provided by experts in the field of record-keeping, financial solvency or security and safety standards which the ICA may accept according to Article 29 (3) UCC IA. In these cases, the submission of a certificate does not mean that the corresponding AEO criterion is automatically fulfilled and not to be checked any more. Rather it is up to the competent customs authority to determine whether and to what extent the criteria are fulfilled.

In this context there are different indicators to be considered for evaluation if and to what extent a certificate or a standard is relevant and substantial and can be helpful within the AEO application procedure. Some of those indicators are:

- who has issued the certificate or who is competent for granting the standard? Is the certificate/authorisation granted by an authority or by a third party? Is the third party internationally accredited?
- in what way the certificate/authorisation is granted? Are there checks done by an authority (examples under [Part 3, Section III, point 4.2. of these Guidelines](#)), by self-assessment of an operator or is there a verification done by an independent and accredited third party?
- was there an on-site audit or documentary verification only?
- what are the reasons for the operator to apply for the certificate/authorisation?

---

<sup>19</sup> MLA (Multilateral Recognition Arrangement) or MRA. See also [www.european-accreditation.org](http://www.european-accreditation.org)

- is the certification/authorisation process done by the company itself or is there a consultant installed by the company?
- is the certificate/authorisation valid for the whole entity, one special site or one single process?
- when was the certificate/authorisation issued? When did the last audit take place? What were the conclusions of the last audit?

The list of known standards and certificates/authorisations presented below is not exhaustive. Due to the variety of economic activities of economic operators and due to national particularities it only includes the most common ones.

It is to be noted that applicants can submit information on every standard they have fulfilled or certificates/authorisations they hold with impact to the AEO criteria to the competent customs authority. Then the competent customs authority will check whether it can be taken into account and to which extent. This is also valid if the economic operator was counselled by an independent authority/institution in cases influencing the AEO criteria without leading to a certification/authorisation (e.g. individual guidance of the local police in crime prevention on site, training programmes).

It should also be noted that it is not necessary, for the purposes of becoming an AEO, to hold any of those certificates/authorisations or to be counselled by third parties. If any certificates/authorisations are available, they could be useful to the customs authorities (see also [SAQ Explanatory Notes](#) for sections 3 and 6 related to accounting and logistical system and to security and safety requirements).

Consider also that it is always the responsibility of the applicant to demonstrate that the AEO-criteria are fulfilled.

### **3.III.4.2. Certificates/authorisations granted by customs or other government authorities**

#### *a) existing customs authorisations*

When an economic operator is applying for an AEO status all other customs authorisations already given to him should be taken into account.

#### *b) certificates granted by aviation agencies or authorities*

Aviation authorities approve entities that are involved in the handling of air cargo. Depending on the role in the supply chain, entities can be granted the status of a RA or RC by the mentioned authorities, while Account Agent (AC) is designated directly by a RA.

RA are companies such as agencies, freight forwarders or other entities that are in business with an airline and carry out security controls, which are recognised or prescribed by the competent authority in respect of cargo, courier and express parcels or mails.

A KC is a consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of cargo or mail on any aircraft.

For a RA and a KC the criteria laid down in Article 28 (1) UCC IA shall be deemed to be met according to Article 28 (3) UCC IA in relation to the premises and the operations concerned for which the economic operator obtained the RA or the KC status. Unlike the AEO programme both, the KC and the RA status are always given to a specific site. It should also be noted that the KC and RA status, in principle, only applies to outgoing goods transported on-board an aircraft. For incoming goods, the processes are not examined and approved.

Comparison carried out by the competent Commission Services in cooperation with EU Member States, between RA, KC and AEO criteria concluded that the requirements of these programmes were in principle comparable in the following four areas:

- Building security
- Appropriate access controls
- Cargo security
- Personnel security

For this reason, in the areas mentioned above it is most likely to find the condition that are common and consequently are deemed to be met.

Therefore, in case the applicant for AEOS has been already approved as a KC or as a RA it should be properly assessed whether the applicant has other business activities and if so, they have to be still examined. There should not be an automatic recognition of the security and safety examinations, but at the same time duplication and re-examination of the same areas and operations should be excluded.

Although there is no legal recognition of the AC status, similar objectives are pursued so that the AC status may be helpful during the AEO authorisation procedure, too.

c) *International Ship and Port Facility Security (ISPS)*

The IMO has adopted as part of the international, mandatory “Safety of Life at Sea Convention (SOLAS)”, an international, mandatory code for the security of ships and port facilities, the International Ship and Port Facility Security Code' (ISPS-Code). It prescribes responsibilities to governments, shipping companies, ship's masters, shipboard personnel, ports, ports facilities and port facility personnel to perform risk assessment and risk analysis, and to develop, maintain and improve security plans for the shipping company and its vessels as well as for ports and port facilities with the aim of preventing security incidents affecting ships or port facilities used in international trade.

The security requirements of the ISPS-Code include physical security measures, including access control to ships and port facilities as well as maintaining the integrity of cargo and cargo units. These measures have to be documented duly in a security plan which is submitted to the Designated Authority for Ship and Port Security. The approved security plan is not only a helpful tool to assess the security criterion for AEO, but shall also, for those elements in the approved security plan that are identical or correspond to the AEO conditions, be considered by Customs as compliance with these conditions (Article 28 (2) UCC IA).

While ships and port facilities meeting the applicable ISPS Code requirements are being issued certificates proving this, it must be noted that shipping companies' compliance with the relevant parts of the ISPS Code is subject to mandatory validation by national maritime administrations in cooperation with the EU's European Maritime Safety Agency (EMSA);



such authoritative validation of the shipping company should therefore also be considered in the context of the AEO authorisation.

d) *Eligibility of the European Central Bank Eurosystem credit assessment framework (ECAAF)*

The European Central Bank Eurosystem credit assessment framework (ECAAF) defines the procedures, rules and techniques which ensure that the Eurosystem requirement of high credit standards for all eligible assets is met. In the assessment of the credit standard the Eurosystem takes into account institutional criteria and features guaranteeing similar protection for the instrument holder such as guarantees. In some member states eligibility is certificated by the national central bank. The Eurosystem's permanent benchmark for establishing its minimum requirements for high credit standards is defined in terms of a "single A" credit assessment, "single A" meaning a minimum long-term rating of "A-" by Standard & Poor's or Fitch Ratings, of "A3" by Moody's, or of "AL" by DBRS.

Therefore the assessment by rating agencies can also be taken into account for the assessment of the criterion on proven financial solvency.

e) *Sarbanes-Oxley-Act (SOX)*

The SOX is a United States federal law, which sets out new or enhances standards for all U.S. public company boards, management and public accounting firms. It is also applicable for companies outside the US, whose stocks are traded in the US. It mainly includes regulations on the internal control system for accounting, balancing and financial report. The focus is on disclosure requirements and the liability of the leadership.

Even if a company is compliant with the SOX regulations there is no automatic fulfilment of any AEO criterion. However, this should be an indicator to be considered in the risk analysis and in the context of the AEO authorisation.

f) *AEO programmes or similar programmes in third countries*

In some countries there is a security and safety programme in place which is in line with the AEO concept of WCO SAFE Framework. Even if there is no mutual recognition between EU and a particular country, the fact that an economic operator is validated/certified under such a programme is also of importance in the context of the AEO authorisation and should be taken into account by the competent customs authority in the examination process for granting an AEO status.

g) *TIR (Transports Internationaux Routiers)*

Under the auspices of the UNECE, the Customs Convention on the International Transport of Goods under Cover of TIR Carnets in 1975 (TIR Convention 1975) was developed.

The TIR Convention is maintained by the UNECE who also maintains the TIR Handbook. The Handbook not only contains the text of the Convention but also a wealth of other useful information concerning the practical application of the Convention.

Of particular interest for the purpose of an AEO authorisation is the controlled access to TIR procedures, which constitutes one of the pillars of the TIR Convention. According to Article 6 of the TIR Convention, the access to TIR procedures shall be granted by competent authorities only to transport operators who fulfil the minimum conditions and requirement laid down in Annex 9, Part 2 to the Convention, namely:

- proven experience and capability to engage in international transport;
- sound financial standing;
- proven knowledge in the application of TIR;
- absence of serious or repeated offences against customs or tax legislation;
- an undertaking in a written declaration of commitment to comply with Customs legislation and to pay the sums due in case of infringement or irregularity.

Of particular interest for the purpose of an AEO authorisation can also be the approval of road vehicles and containers. The TIR Convention stipulates that goods shall be carried in containers or road vehicles the load compartments of which are so constructed that there shall be no access to the interior when secured by seal. If a container or load compartment fulfils the requirements of the Convention, relevant national approval or inspection authorities issue so called approval certificates for road vehicles or containers.

#### h) *Others*

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

### **3.III.4.3 Commercial standards and certifications**

#### a) Certificates according to ISO 27001

The ISO 27001 is a worldwide standard by the ISO for the safety of information technology and the protection set of electronic information systems. This standard includes regulations on information technology, security technology and information security management systems requirements. It specifies the requirements for production, introduction, monitoring, maintenance and improvement of documented information security management system. So an ISO 27001 certification is applicable to different sectors, e.g. wording of requirements and aims for information security, cost efficient management of safety risks, ensure the compliance with law and regulations.

#### b) ISO 9001:2015 (if any combined with ISO 14001:2009)

The ISO 9001 standard created by the ISO includes substantial proposals for the improvement of quality management in enterprises. The purpose of this standard is to increase the effectiveness of the company and the improvement of quality assurance. Therefore, the customer requirements should be met with a certain quality process. Ultimately, customer satisfaction should be increased.

For the AEO application procedure an ISO 9001:2015 certification can be useful e.g. for the assessment of the internal control system.

#### c) ISO 28000:2007

Pursuant to ISO 28000:2007, companies can be certified as having an adequate security management system regarding the security of the international supply chain. ISO 28000:2007

is a framework standard and the requirements for security and safety in this particular standard are very general.

However, another ISO standard in the ISO 28000 series, ISO 28001:2007, includes much more specific supply chain security requirements and aims to be aligned with the WCO SAFE's AEO criteria. Compliance with ISO 28001 should therefore, according to Article 28 (2) UCC IA, be considered by the customs authorities in the context of the AEO authorisation.

#### d) TAPA Certificates

TAPA is an incorporation of persons responsible for security and logistics in the fields of production and logistics. The aim of this international association is to protect their especially high-priced goods against theft and loss during storage, transshipment and transport. TAPA certificates are granted on the basis of cargo security standards developed by the TAPA organisation. Hereby, checks concerning compliance with the standards are done by a neutral certification body (TAPA certificates A or B) or in a self-assessment by the company (TAPA certificate C). The TAPA cargo security standards include instructions for security concerning buildings, equipment and processes during storage and transportation of goods.

A successful certification (certificates A and B) according to the requirements of the cargo security standards by the TAPA organisation requires adherence to a high level of physical security standards by the certificate holder.

However, it remains important to note that TAPA certificates are being issued for individual sites and not for the whole company.

### **3.III.5. Parent/subsidiary companies with common system/procedures**

Regardless of the legal set-up of a particular company, the relevant criteria have to be fulfilled in principal by the applicant.

The particularities in the event of outsourced activities have already been explained in [Part 2 'AEO criteria' of these Guidelines](#). The same principles are applicable if activities are outsourced within a group of affiliated companies.

However, in terms of parent/subsidiary companies there are some factors to be considered, which can influence the risk analysis and the audit process. First, the connection has to be clarified and if it has influence on administrative and/or operative processes.

There are cases in which a subsidiary will be granted independence by the parent company. Frequently there are at least profit transfer agreements or the like between affiliated companies. In some cases specific activities are outsourced within the group by a contract, which can lead towards a company without own personnel at all.

In other cases specialised units fulfil tasks (shared services) for all companies belonging to a group.

In all these cases the connection can influence the likelihood of a risk to occur and the impact of the occurring risk both positive and negative.

It might be of practical importance for the examination of the AEO application that in case of common processes of connected companies, it will be often sufficient to check these processes only once.

This is also relevant if one unit within the group conducts particular activities for all affiliated companies (shared services) as if different legal entities within one group make use of the same principles (corporate standards).

This can speed up the audit process and the specialist knowledge can also enhance the quality of processes. At the same time knowledge about one company of a group has always also to be assessed in the light of a possible impact on affiliated companies. If the internal control system fails in one affiliated company with common corporate standards, the internal control system in the connected companies should not be automatically assumed to also have failed, but the customs authorities should consider to review those other systems (wholly or in part).

### **3.III.6. Risk and risk analysis**

#### **3.III.6.1 Economic operator's risk assessment and management**

The organisation of an economic operator can be a complex system involving many interrelated processes. An AEO should focus on processes, management of risk, internal controls and measures taken to reduce risks. This should include a regular review of those processes, controls and measures taken to reduce or mitigate risks related to the international movement of goods. Internal control is the process implemented by the economic operator to prevent, detect, and address risks in order to assure that all relevant processes are adequate. An organisation that has not implemented any internal control system or there is evidence that the system is performing poorly is by definition at risk.

Risk based management systems are the disciplines by which economic operators in any industry assess, control, monitor and address risks. For an AEO, this means that the economic operator has to set out clearly in its policies/strategies the objectives of being compliant with customs rules and of securing its part of the supply chain according to its business model. The management system should allow for:

- a continual cycle of identifying needs or requirements,
- evaluating the best means for complying with the requirements,
- implementing a managed process for applying the selected management actions,
- monitoring the performance of the system,
- maintaining evidence of the application of processes used to meet business objectives, and identify functional or business improvement opportunities, including reporting mechanisms on gaps, incidental mistakes and possible structural errors.

This all has to be seen within the framework of complying with the legal and regulatory requirements to which the organisation subscribes or is required to comply.

The more an organisation is aware about its processes and the risks related to its activities, the more it is possible that processes can be managed accordingly. This means that an organisation should be aware about concepts such as: risk management; governance; control (monitoring, re-assessment; re-implement process and/or redesign procedures) and have implemented the relevant procedures to cover the most important risks and identify new risks.

Within the economic operator organisation there should be a responsible person or, depending on its size and complexity, a unit responsible for carrying out risk and threat assessment and for putting in place and evaluating the internal controls and other measures. Risk and threat

assessment should cover all the risks relevant for the AEO status keeping into account the role of the economic operator in the supply chain and should include:

- security/safety threats to premises and goods;
- fiscal threats;
- reliability of information related to customs operations and logistics of goods;
- visible audit trail and prevention and detection of fraud and errors;
- contractual arrangements for business partners in the supply chain.

The risk and threat assessment for security and safety purposes should cover all the premises which are relevant to the economic operator's customs related activities.

### **3.III.6.2. Customs risk analysis and auditing**

As seen under the previous point, the economic operator is the one that is in the best position to assess his own risks and to take action to cover them. Customs' role is to perform audits to assess how effectively the economic operator tackles these issues. Is the applicant aware of the most important risks and is he or she taking adequate measures to cover them?

To carry out this evaluation and take the appropriate decision whether to grant the AEO status or not, customs authorities have to:

- assess the risk of the economic operator;
- prepare an adequate audit plan based on risk;
- perform the audit;
- address any non-acceptable risk with the economic operator;
- take the appropriate decision, either granting the AEO status or not;
- monitor, and if necessary re-assess, the economic operator concerned.

The economic operator should have implemented adequate procedures and measures at management level to deal with the risk relevant for the AEO authorisation. In this context the economic operator should be aware that it is possible to outsource "activities" but not "responsibilities". In the context of the AEO concept, the economic operator should be aware of the risks related to outsourcing activities and should take action to cover these risks and provide evidence to customs about that.

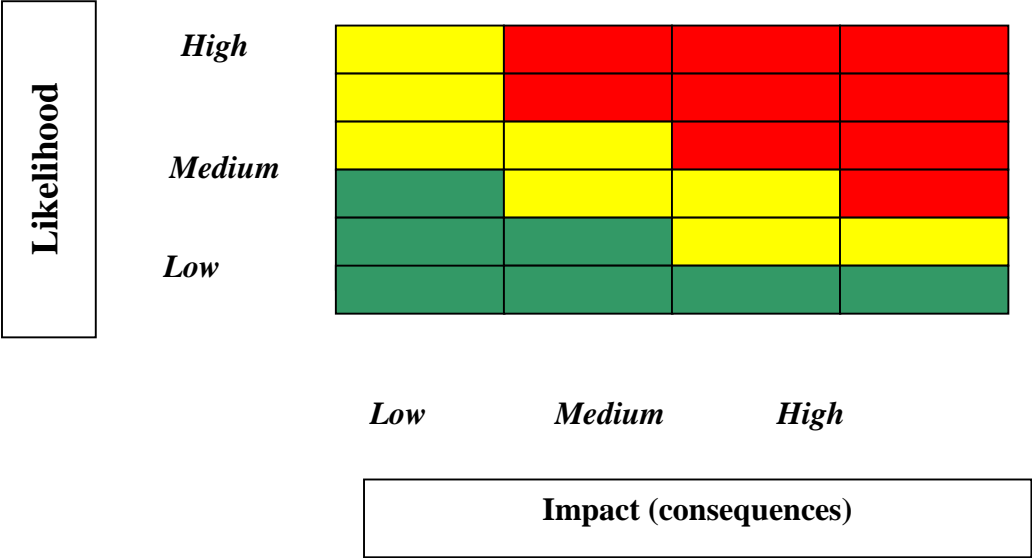
#### Risk assessment of a specific economic operator

For customs the first step is to collect as much relevant information as possible to understand the economic operator's business (see Part 3, Section 3.III.1). Once this has been done customs can proceed with the risk assessment, elaborating an audit plan and conducting the audit. Using all available information a risk assessment is undertaken on all the relevant risk area of the operator's activity within the international supply chain in accordance with the economic operator's business model. This is to be done area by area, taking into consideration all risks related to the activity of the economic operator and relevant for the AEO status. At this stage this is the risk as assessed based on all available information before the audit and on the estimated existence and effectiveness of the internal control system in the economic operator's organisation. It should guide auditors in preparing the audit plan.

#### Risk Mapping and AEO COMPACT Model

In the WCO "Risk management guide", the risk from a customs perspective is generally defined as: "The potential for non-compliance with Customs laws", but in the context of these guidelines it appears better to have a broader approach and define the risk as "the probability

that an action or event will adversely affect an organisation’s ability to be compliant with the AEO requirements and criteria”. There are two things to be considered: the likelihood that an event occurs but also its impact, and in order to assess the importance of the relevant risk, these two dimensions should always be taken into account. These concepts can be visualised through the so called risk matrix in the following picture:



A risk can never be totally eliminated, except when a process is aborted totally. This matrix shows a high consequence risk would be unacceptable in all but a low likelihood situation, while a medium consequence risk would be unacceptable in a high likelihood situation. The aim is to reduce the level of risk (impact/likelihood) to an acceptable level, and assure through monitoring that it is not changing.

Normally, it should be considered that if:

- the risk is in the red area, it is considered high and further countermeasures should be introduced to reduce the level of risk;
- the risk is in the yellow area, corrective actions can be suggested to move the risk in the green area, either mitigating the impact or reducing the probability that it occurs;
- the risk is in the green area, the risk can be treated as acceptable but improvements can be considered.

These two dimensions should also be used to prioritise risks and envisage appropriate countermeasures.

It is clear that the risks could have different relevance depending on the perspective of a specific stakeholder concerned. For example, an economic operator and customs authorities could have a different understanding of the concept of security: the objective of the economic operator could be to secure the cargo against the risk of theft, while customs’ focus will be on protecting citizens and preventing the insertion of illicit or dangerous goods into the supply chain. It is important that the economic operator’s threat and risk assessment cover all risks to their business relevant for the AEO status, keeping in mind the scope of the AEO concept and the economic operators’ role in the international supply chain in accordance with its business model.

As part of the process the economic operator not only has to implement and manage appropriate selected measures but also to make sure that the measures work and review and reassess them.

This means the economic operator should monitor on a regular basis the relevant processes, checking whether the procedures in place are adequate to assure customs and security and safety compliance. The economic operator should document what has been done, both to manage the improvement action and to evidence it to customs authorities.

Summarising, the economic operator should have in place procedures and measures to:

- clearly set out the assets and objectives at stake (i.e. for AEO it is clear that what is important is to have the objective of being compliant with the customs rules and securing its supply chain);
- identify the threats that can put in danger assets and objectives set out;
- continuously monitor whether its own assets are threatened by those identified threats;
- assess the risk related to his or her role in the international supply chain in accordance with its business model;
- cover this risks by taking action and implementing adequate procedures; and
- monitor the effectiveness of the procedures implemented.

In order to have comparable results the risk assessment process should be based on a recognised risk analysis model. The AEO COMPACT Model<sup>20</sup> is recommended to be used.

### **3.III.7. Auditing and risk based audit**

#### **3.III.7.1. Preparing an audit plan**

The auditor has the responsibility to plan and perform the audit to obtain reasonable assurance whether the economic operator is compliant with the established criteria. The auditors should determine an audit plan according to the risks identified for the specific economic operator.

This **audit plan** shall be the specific guideline to be followed when conducting the audit and shall specify objectives, scope and methods of the audit.

The audit plan should be drawn as a result of the risk assessment and reflect information about:

- the risks of each area, indicating the relevant points/aspects to check;
- a Risk Analysis Matrix;
- departments or units to be scrutinised;
- the management and the staff to interview;
- what, how and when a specific transaction/security tests should be done.

Auditing action and allocated resources should be based on the following principle: “the higher the risk the higher the level of scrutiny”.

---

<sup>20</sup> Authorised Economic Operator, Compliance and Partnership Customs and Trade (TAXUD/2006/1452)

### **3.III.7.2. Perform auditing activities**

Auditing is a systematic process of objectively obtaining and evaluating evidence. It includes also communicating the results to continuously improve the relevant processes and, in doing so, reduce or mitigate the risk related to the specific activities carried out by the operator to an acceptable level. A key element of the audit is to assess the effectiveness of the economic operator's risk assessment and internal controls. The economic operator should have committed to assess, reduce and mitigate the risks identified to its business and to document this. It is also important to bear in mind that for SME's the level of internal control and documentation required should be appropriate in relation to the level of risk depending on the scope and size of their business. However, even where economic operators have carried out a risk assessment, their assessment may not always correspond with the threats and risks identified by customs authorities.

Audit should always be risk-based and focused on high risk areas to be able to meet the objectives of the audit in relation to the particular economic operator. Risk-based audit (RBA) is an approach to audit that analyses audit risks, sets acceptable thresholds based on audit risk analysis and develops audit programmes that allocate a larger portion of audit resources to high-risk areas. This is important because an auditor may not be able to perform detailed audit procedures on all areas of audit, particularly in the case of large multinationals (i.e. in cases of many premises). Audit should focus primarily on the identification and assessment of the highest risks and the internal controls and counter and mitigating measures taken by the applicant and provide a framework to reduce the impact of these identified risks to an acceptable level before granting the AEO status. RBA is primarily characterised as systems audit.

### **3.III.7.3. Managing residual risk**

RBA provides indicators of risks as a basis of opportunities for improvement of audited risk management and control processes. This gives an opportunity to the economic operator to improve its operations from recommendations on risks that do not have current impact in terms both of customs compliance and security and safety, but could put in danger the economic operator's operational strategies and performance in the long run. A good risk analysis provides a framework for assurance in performance auditing.

Auditors should take into account that the audit plan is a living document that can change according to the information auditors receive during the audit. A potential risk estimated low in the risk assessment phase can be reassessed as high once the actual process is observed and the procedures are judged not only on paper but also how they have been implemented.

The auditors should always evaluate any additional information related to the areas judged as being in the "green area" and be ready to check the relevant procedures in case the estimated risk is challenged by facts.

The use of the table 'Threats, risks and possible solutions', attached as [Annex 2 to these Guidelines](#) is recommended.



RBA consists of four main phases starting with the identification and prioritisation of risks, to the determination of residual risk, reduction of residual risk to acceptable level and the reporting of audit results to the economic operator. These are achieved through the following:

- establish the various operations of the economic operator in order to identify and prioritise risks, including examining their security plan if there is such and threat assessment and identifying the measures taken and internal controls;
- confirm economic operator's management strategies and procedures and evaluate controls to determine residual audit risk. Where appropriate test those controls;
- manage any residual risk to reduce it to acceptable level (follow up action should be agreed with the economic operator in order to reduce the impact and/or likelihood of a specific risk and have all the risks in the green area);
- inform the economic operator of audit results. It is important that auditors clearly indicate to the applicant any risks identified including also recommendations on how they can be overcome;
- monitoring and, if necessary, re-assess criteria and requirements.

#### **3.III.7.4. Final report and audit documentation**

The verification and checks carried out during the audit and the conclusions of the auditors should be accurately documented. It is necessary to document what has been done and not just collect evidence and information. This is important both for customs authorities throughout the authorisation process including the management of the authorisation and also for the economic operator.

The final report and the audit documentation should include the following information in a clear and systematic way:

- a clear overview of the economic operator (its business, its role in the supply chain, its business model, its customs related activities, etc.);
- a clear and accurate description of what has been done to verify the fulfilment of the AEO criteria;
- a clear description of all risk areas considered and checked and any follow-up actions suggested to the applicant;
- a clear report of any action or reaction the applicant has undertaken or expressed to the auditors;
- the clear recommendation about whether to grant the status or not according to the result of auditing activities;
- in case the AEO status is not granted, complete and detailed justifications why the status is not granted, including any information received from other Member States, stating whether they have been obtained through the “information” and/or “consultation” procedure;
- an overview regarding the AEO risk profile and in case the AEO status is granted any recommendations for monitoring and/or re-assessment (see [Part 5 'Management of the authorisation' of these Guidelines](#)).

Therefore, the final report and audit documentation are a highly important documents reflecting the overall work already done (risk analysis, audit planning, checks and visits to the

premises of the applicant, information received by other Member States, risk profile of the specific economic operator, etc.) in a summarised and systemised way and providing clear indications about future actions. |

Before the final report and audit documentation are written, in case of any unclarity the auditor should reconfirm with the economic operator the facts described in the report.

## **Section IV - Decision about granting of the status**

### **3.IV.1. Factors to be considered before taking the decision**

The decision of the customs authorities on if the AEO status can be granted or not is based on the information collected and analysed through the different stages of the authorisation process, from receipt of the application submitted to when the audit process has been fully completed.

To enable customs authorities to take the decision, the following factors should be taken into consideration:

- all previous information known about the applicant by the competent authority, including the AEO application form along with the completed [SAQ](#), and all other supporting information. This information may need to be rechecked and, in some cases, updated, in order to take account of possible changes, which may have occurred in the period from the date of receipt and acceptance of the application to the end of the authorisation process and issuing the final decision.
- all relevant conclusions drawn by the auditors during the audit process. Customs authorities should prepare and implement the most efficient methods of internal communication of the audit results which have emanated from the audit team(s) to the other competent customs authorities involved in taking the decision. A full documentation of the checks done through and audit report or other appropriate document/way is recommended as the most appropriate mechanism to do so;
- the results of any other evaluation of the organisation and procedures of the applicant that took place for other control reasons.

At the end of the process and before taking the final decision, the ICA will inform the applicant in particular where those conclusions are likely to result in a negative decision. In that case opportunity shall be given to the applicant to express his or her point of view, respond to the envisaged decision and provide supplementary information with the intention of achieving a positive decision (Article 22(6) UCC).

To avoid that the right to be heard results in prolonged delays, Articles 8 (1) and 13 (2) UCC DA define a period of 30 days. The applicant should be advised that failure to respond within that period will be deemed to be a waiver of the right to be heard. In circumstances where a person indicates that they wish to waive the right to be heard, this fact should be recorded and retained as evidence that the applicant was provided with the possibility to respond.

The applicant will be informed whether customs authorities decide or not to alter the original decision on the basis of the supplementary information provided.

### **3.IV.2. Taking the decision**

The following factors have to be taken into consideration:

- each Member State determines, within its internal organisation, the specific service of the organisation which has the competence to decide on whether to grant the AEO status or not;
- when the decision is taken the final report of the competent audit team(s) should play an essential role in relation to the compliance or not with the specific AEO criteria, as detailed above;
- Member States have 120 calendar days to take the decision (Article 22(3) UCC). This time-limit can be extended in the following cases:
  - by the ICA by another 60 calendar days, if it is unable to meet the 120 calendar days. The applicant has to be informed about the extension before the expiry of the 120 calendar days (Article 28 (1) UCC DA);
  - on request by the applicant and subject to agreement with the customs authority concerned. During the latter extension, the applicant carries out adjustments in order to satisfy the criteria and communicates them to the customs authority. The period of extension requested should be reasonable with a view to the nature of the adjustments to be done (Article 22 (3) third subparagraph UCC);
  - by the ICA in case of request of necessary additional information from the applicant. The applicant shall provide the information within 30 days maximum by the request. The applicant shall be informed of the extension of the time-limit for taking a decision. (Article 13 (1) UCC DA);
  - by the ICA by a period of 30 days, in case the right to be heard is granted to the applicant. The applicant shall be informed of the extension. (Article 13 (2) UCC DA);
  - by the ICA, where the ICA has extended the period for consultation of another customs authority. The time-limit for taking the decision shall be extended by the same period of time as the extension of the consultation period. The applicant shall be informed of the extension of the time-limit for taking a decision (Article 13 (3) UCC DA);
  - by the ICA, if customs authorities are conducting investigations based on serious grounds for suspecting an infringement of customs legislation. Such an extension shall not exceed nine months. Unless it would jeopardise the investigations, the applicant shall be informed about the extension (Article 13 (4) UCC DA);
  - by the ICA, where criminal proceedings are pending which gives rise to doubts whether the applicant, or if applicable the persons listed in Article 24 (1) (a), (b) and (c) UCC IA, fulfils the conditions related to compliance with customs legislation and taxation rules and there is no record of serious criminal offences relating to its economic activity. The extension of the period to take the decision shall be extended by the time necessary to complete those proceedings (Article 28 (2) UCC DA).

### **3.IV.3. Informing the applicant**

The applicant shall be informed in writing about the following situations:

- the acceptance of the application (Article 22 (2) second sub-paragraph UCC);
- the extension of the period for taking of a decision provided by Article 28 UCC DA;
- the extended period for taking a decision due to investigations by the customs authorities unless it would jeopardise those investigations (Article 13 (4) last sentence UCC DA);
- the extended period for taking a decision for consultation (Article 13 (3) UCC DA);
- the extended period for taking a decision due to the request of additional information (Article 13(1) UCC DA);
- the extended period due to the applicant of the right to be heard (Article 13(2) UCC DA);
- even if not expressly requested by the legislation it would be appropriate to inform the applicant also in cases where the applicant requests an extension to carry out adjustments in order to ensure the fulfilment of the conditions and criteria (Article 22 (3) third subparagraph UCC);
- even if not expressly requested by the legislation it would be appropriate to inform the applicant also about the extended period for taking a decision where criminal proceedings are pending (Article 28(2) UCC DA).

The ICA shall also inform the applicant about the final decision regarding its application. In this context it is to be noted that any decision to reject an application shall include the reasons for rejection and the right to appeal as provided for in Article 44 UCC. Before the acceptance of the decision to reject an application an opportunity to express economic operator's opinion shall be given (Article 22 (6) UCC).

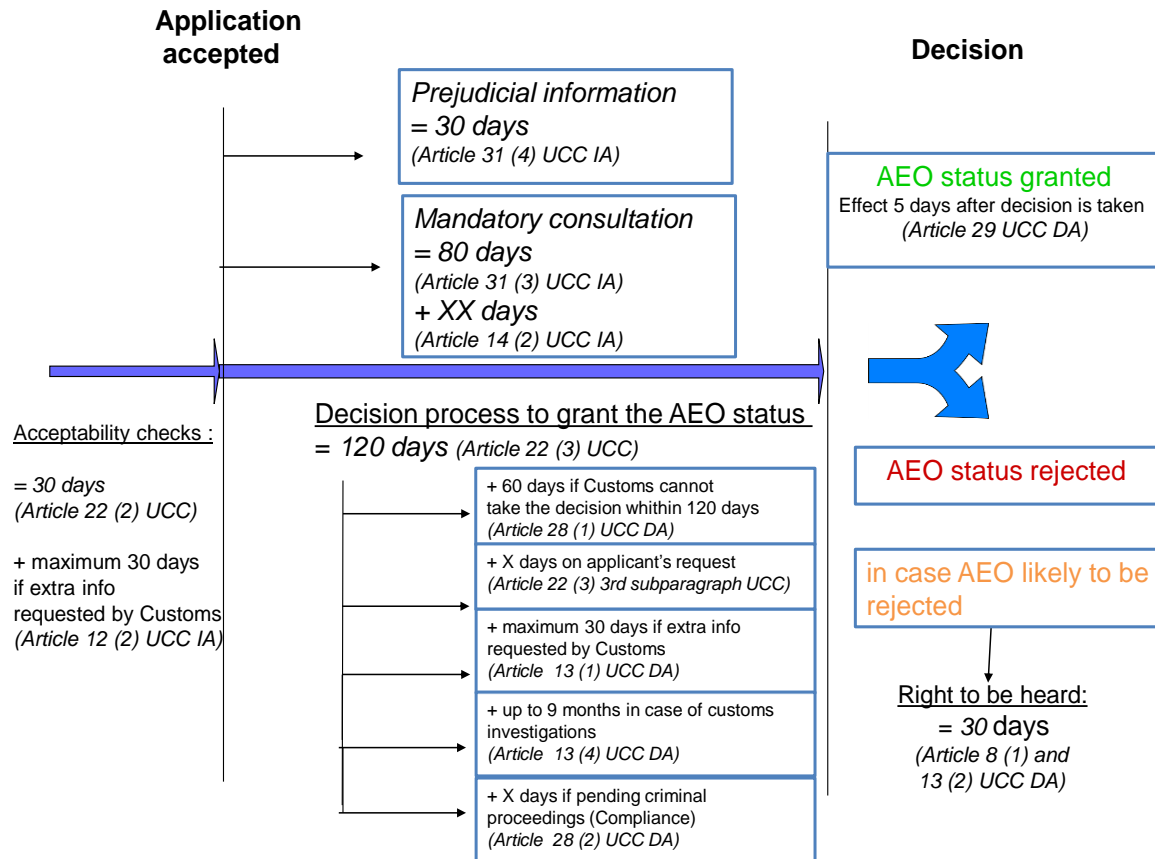
Customs authorities shall inform the economic operator in writing by any relevant means (e.g. by an IT system, by email, by a formal letter etc.).

#### **3.IV.4. Appeals**

Article 44 UCC, provides that *"any person shall have the right to appeal against any decision taken by the customs authorities relating to the application of the customs legislation which concerns him or her directly and individually"*. The person appealing a customs matter should submit the appeal in the format and according to the rules laid down in national legislation.

### 3.IV.5. Time-limits

The following visual presentation provides an overview of the main time-limits in the decision taking process:



## **PART 4, Exchange of information between Member States and with other government authorities**

### **Section 1 - Exchange of information between Member States**

In the context of the AEO procedure, exchange of information between Member States is an important factor when it comes to assuring the compliance of an economic operator with the AEO criteria. This is particularly important because, once granted, the AEO authorisation is valid throughout the EU. It also recognises that many economic operators are engaged in customs activities in a number of different Member States across the EU and the assessment of the AEO criteria should be made against all their relevant customs activities. This can only be done through effective information and consultation procedures between the Member States.

The legislation assigns a leading role to the ICA that is responsible for accepting the application and granting the AEO authorisation. Nevertheless, customs authorities in the other Member States also play an important role in the process. Two different procedures are established in order to exchange information among Member States and provide to the ICA all the relevant information for taking the appropriate decision.

#### **4.I.1. Information procedure**

According to Article 30 (1) UCC IA the ICA shall make information available to the customs authorities of the other Member States without delay and at the latest within 7 days from the date of the acceptance of the application. This will make the other Member States aware that a specific application has been accepted. Thus they can react in case they have at their disposal relevant information for that particular applicant or in case they have been asked by the ICA to take particular action (consultation procedure).

This has to be done through the electronic system "EOS", which is defined in Article 30 UCC IA. Member States are encouraged to ensure that regular checks are carried out in the system to guarantee that they are aware of any applications in which they may have interest. It is recommended that at least weekly checks in the system are performed.

It is also important that each customs authority should also carry out checks in EOS to see whether there is any relevant information to be sent to the ICA or not. Any relevant information about the applicant, related to the compliance with the AEO criteria shall be communicated to the ICA to enable them to make the correct decision based on all available facts. Article 31 (4) UCC IA allows Member States a maximum of 30 calendar days starting from the date of the communication of the application through the EOS system, to make this information available to the ICA. The timely exchanges of information could save Member States valuable time and resources.

The information above is normally submitted before the authorisation has been issued; nevertheless the procedure is available to exchange information at any time, even after the authorisation has been issued. If a Member State has any new information, it has to send it as soon as possible to the ICA as it could have an impact on the conditions to be met by the AEO. This is possible as Article 35 UCC IA foresees that the customs authorities (both the

ICA and other customs authorities) have to monitor the compliance with the conditions and criteria. In case the information sent appears to be relevant and significant, this can lead the ICA to start a re-assessment process according to 15 (1) UCC DA.

The ICA shall take into account the information received either during the authorisation phase or during the monitoring of an authorisation.

#### **4.I.2. Consultation procedure**

According to Article 31 (1) UCC IA *"the customs authority competent to take the decision may consult customs authorities of other Member States which are competent for the place where necessary information is held or where checks have to be carried out for the purpose of examining one or more of the criteria laid down in Article 39 of the Code"*.

As in the case of the information procedure, also the consultation procedure is normally initiated by the ICA at the beginning of the process in order to get information before the authorisation has been issued. Nevertheless, this procedure can be initiated at any time the ICA considers it necessary in order to assess whether the AEO is still compliant or not. The procedure is also to be used during monitorings (Article 14 (4) UCC IA). In particular, when the ICA decides to initiate a re-assessment, it has to decide if the consultation with another (or several) Member State(s) is necessary or not. If deemed necessary, the ICA starts a consultation and waits for the results; otherwise it continues the re-assessment itself and all results (suspensions, revocations, AEO authorisations still valid) will be notified to all Member States when the results are entered into the EOS system.

Following Article 31 (2) UCC IA this consultation shall be mandatory, where

- *the application for the status of AEO is submitted in accordance with Article 12 (1) UCC DA, to the customs authority of the place where the applicant's main accounts for customs purposes are held or are accessible;*
- *the application for the status of AEO is submitted in accordance with Article 27 UCC DA to the customs authority of the Member States where the applicant has a permanent business establishment and where the information about its general logistical management activities in the Union is kept or is accessible;*
- *a part of the records and documentation of relevance for the application for the status of AEO is kept in a Member State other than the one of the customs authority competent to take a decision;*
- *the applicant for the status of AEO maintains a storage facility or has other customs-related activities in a Member State other than the one of the competent customs authority.*

For example it is necessary, to start a consultation procedure if the economic operator has one or more premises with customs-related activities in another Member State; if part of its customs activities is carried out in other Member States; or to get information on some important management member normally resident in other Member States etc. This consultation is mandatory and the consulted customs authority shall reply to the ICA even if the outcome is positive and the applicant meets the criteria requested to be checked. This then ensures that the ICA has the relevant information to support the final decision.

The answer of the consulted Member States should duly be taken into account by the ICA, which has the overall picture of the applicant and is competent to take the decision on the fulfilment of the criteria for the whole business of the economic operator.

There may be cases where the consulted Member State considers the criteria not to be met but the following clarification of the applicant seems to be sufficient for the ICA. In that case the involved Member State should be consulted again.

If no reply is received within the deadline, the ICA will assume that the criterion or criteria for which the consultation has been requested in the consulted Member State are met (Article 14 (3) UCC IA).

According to Article 31 (3) UCC IA *"the customs authorities shall complete the consultation process within 80 days from the date on which the customs authority competent to take the decision communicates the necessary conditions and criteria which have to be examined by the consulted customs authority"*.

According to Article 14 (2) UCC IA, the time-limit for consultation can be extended in any of the following cases:

- (a) where due to the nature of the examinations to be performed the consulted authority requests more time;
- (b) on request by the applicant to the consulted customs authority and subject to agreement of the consulting customs authority. During this extension, the applicant carries out necessary adjustments in order to comply with AEO criteria and is obliged to communicate them to the consulted customs authority.

The time-limits for a consultation, the extension of the time-limit and the conclusion in case of not answering a consultation may also be applied for the purposes of re-assessment and monitoring of a decision due to Article 14 (4) UCC IA.

#### **4.I.3. Means of communication**

All the information related to both the "information procedure" and the "consultation procedure" should be primarily provided using the EOS system through the use of the appropriate codes.

Nevertheless, there are cases where the necessary information cannot be exchanged via EOS. In order to decide how to proceed, it is important to consider whether the relevant information is sensitive or not. Besides, there are cases where the information is not sensitive but due to its format it cannot be codified and as such cannot be exchanged via EOS (unstructured information, attachments, etc.). In these cases Member States can use all available communication channels, including the AEO network contacts.

In other cases the information is of sensitive nature but still cannot be exchanged via EOS, although secure, due to its format. Examples of such cases can be: suspected involvement of the AEO in some not legitimate activities, specific risks related to the AEO, or any other issue



for which any disclosure of the relevant information can result in problems either for the customs (jeopardise check and controls) or for the economic operator.

With regard to sensitive type of information which cannot be exchanged via EOS due to its format, CRMS (Customs Risk Management System) should be used.

It has also to be noted, that the ICA has to write a justified administrative act to the economic operator in case of a negative decision. Therefore, in case the consulted customs authority establishes that the applicant does not fulfil one or more of the conditions and criteria for taking a favourable decision, the results, duly documented and justified, shall be transmitted to the ICA (Art 14 (1) second subparagraph UCC IA).

## **Section II – Exchange of information between customs and other government authorities**

In the framework of the AEO authorisation process, consultation and where appropriate exchange of information between customs and other government authorities is very important. Depending on the specific case and the respective legislation regulating it the level and form of consultation and/or exchange of information with other government authorities can be different.

The first case is the general condition as specified in Article 38 (1) UCC that the AEO status is granted by customs authorities following consultation with other competent authorities. The necessity for such a consultation depends on a number of issues, e.g. type of economic activity of the applicant and goods involved; possibility of checks by customs authorities based on the information available to them in order to establish whether the applicant complies with any obligations he or she might have under other relevant legislation (e.g. commercial policy measures, specific prohibitions and restrictions).

The second case where exchange of information with other competent authorities is necessary when other Union legislation provides for recognition of the AEO status. In these cases it is also the customs legislation that defines who these competent authorities are and the cases where exchange of information with them is obligatory in order to ensure the proper implementation of the respective recognition envisaged.

A third case could be, that the data exchange is based on national level to enhance the quality of the pending AEO authorisation and the authorisation/certificate issued by the other competent government authority and/or to avoid unnecessary double checks for the economic operator.

### **(a) Information to be exchanged from customs authorities to the appropriate national authority responsible for civil aviation security**

Article 35 (4) UCC IA lays down that *"where the AEOS is a regulated agent or a known consignor as defined in Article 3 of Regulation (EC) No 300/2008 and fulfils the requirements laid down in Commission Implementing Regulation (EU) 2015/1998, the competent customs authority shall immediately make available to the appropriate national authority responsible*

*for civil aviation security the following minimum information related to the AEO status which it has at its disposal:*

*the AEOS authorisation, including the name of the holder of the authorisation and, where applicable, its amendment or revocation or the suspension of the status of authorised economic operator and the reasons therefor;*

*information about whether the specific site concerned has been visited by customs authorities, the date of the last visit, and whether the visit took place with a view to the authorisation process, re-assessment or monitoring;*

*any re-assessments of the AEOS authorisation and the results thereof.*

*The national customs authorities shall, in agreement with the appropriate national authority responsible for civil aviation security, establish detailed modalities for the exchange of any information which is not covered by the electronic system referred to in Article 30" UCC IA.*

Where applicable, in particular when AEO status is a basis for the grant of approval, according to Article 30 (2) UCC IA *"the competent customs authority may grant access to the EOS system to the appropriate national authority responsible for civil aviation security. The access shall be related to the following information:*

(a) *the AEOS authorisations, including the name of the holder of the authorisation and, where applicable, their amendment or revocation or the suspension of the status of authorised economic operator and the reasons therefor;*

(b) *any re-assessments of AEOS authorisations and the results thereof.*

*The national authorities responsible for civil aviation security handling the information concerned shall use it only for the purposes of the relevant programmes for regulated agent or known consignor and shall implement appropriate technical and organisational measures to ensure the security of this information".*

#### **(b) Information to be exchanged from the appropriate national authority responsible for civil aviation security to customs authorities**

Exchange of information is necessary also from the appropriate national authority responsible for civil aviation security to the national customs authorities to ensure that the status of regulated agent or known consignor and any changes thereof are appropriately considered for the purposes of granting and managing of the AEO status.

Points 6.3.1.8 and 6.4.1.7 of the Annex to the Commission Implementing Regulation (EU) 2015/1998 envisage that the appropriate authority shall make available to the customs authority any information related to the status of regulated agent or known consignor which could be relevant in respect of holding the AEOS authorisation.

The modalities for the exchange of this information shall be established and agreed between customs authorities and the appropriate national aviation authority.

#### **(c) Other areas of information exchange**

The customs authorities may take into consideration the results of assessments or audits carried out in accordance with Union legislation to the extent they are relevant for the examination of the criteria.

An example for the data exchange for the benefit of customs, other government authorities and the economic operator is the information on the Internal Compliance Programme (ICP) relevant for purposes of dual use goods which has a comparable objective as the AEO programme.

The national authorities who grant licenses for dual use goods and the national customs authorities are encouraged to exchange information on AEO authorised companies and holders of Global export authorisations, if national legislation allows so.

## **PART 5, Management of the authorisation**

### **Section I - Monitoring**

#### **5.I.1. General**

Monitoring by the economic operator and obligation to notify of any changes

Regular monitoring is the primary responsibility of the economic operator. It should form part of its internal control systems. The economic operator should be able to demonstrate how the monitoring is performed and show the results. The economic operator should review its processes, risks and systems to reflect any significant changes in its operations. Customs authorities should be informed about these changes.

There is also a legal requirement laid down in Article 23 (2) UCC that the holder of the AEO authorisation shall inform the customs authorities without delay of any factor arising after the decision was taken, which may influence its continuation or content. Although, it depends very much on the particular AEO concerned and thus the list cannot be exhaustive, [Annex 4 of these Guidelines](#) provides examples of cases where customs should be informed.

The AEO shall inform the issuing customs authority of any changes related to any other relevant approval, authorisation or certification granted by other government authorities that may have an impact on the AEO authorisation (e.g. withdrawal of a RA or KC status).

The AEO shall ensure it holds the original documentation, including documented findings and reports from revalidations as this may be requested by customs authorities.

To ensure AEOs are aware of this obligation the competent customs authority may e.g.:

- give examples of information which should be communicated to the competent customs authority in the written decision, letter etc. which is sent to the AEO after issue of the AEO authorisation, in this context [Annex 4 to these Guidelines](#) could provide as a helping tool;
- provide the AEO with the relevant contact point within the customs administration for communication of all information related to its authorisation;

- send an e-mail message (e.g. in the e-mail with which Customs provide the AEO logo to the economic operator) to the AEO contact person in the company stressing this obligation and giving the possibility to communicate relevant changes;
- when an unannounced change is discovered by customs officers, send a “warning” e-mail to the AEO contact person in the company pointing out that this kind of information has to be communicated to the competent customs authority;
- sending regularly (e.g. annually) a short questionnaire “reminder” (using some questions from [SAQ](#)) to the AEO contact person (via e-mail) asking about possible changes regarding relevant criteria.

### Monitoring by the customs authorities

Monitoring is done on a continuous basis by the customs authorities, including through monitoring of the day-to-day activities of the AEO and visits to the premises. It aims at the early detection of any signal of non-compliance and shall lead to prompt action in case difficulties or non-compliance are detected.

According to Article 23 (5) and 38 (1) UCC, the AEO status is subject to monitoring. Furthermore, taking into consideration that the period of validity of the AEO authorisation is not limited it is of great importance that the criteria and conditions of the AEO status are evaluated on a regular basis.

At the same time, 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.

Thus, it is significant for the competent customs authority to ensure that a system for monitoring the compliance with the conditions and criteria of the authorisation is developed in conjunction with the AEO. Any control measures undertaken by the customs authorities should be recorded.

According to Article 35 UCC IA, *"the customs authorities of the Member States shall inform the competent customs authority without delay of any factors arising after the grant of the status of AEO which may influence its continuation or content.*

*The competent customs authority shall make available all relevant information at its disposal to the customs authorities of the other Member States where the AEO carries out customs-related activities. Where a customs authority revokes a favourable decision which has been taken on the basis of the status of AEO, it shall notify the customs authority which granted the status.*

*Where the AEO is a regulated agent or a known consignor as defined in Article 3 of Regulation (EC) No 300/2008 and fulfils the requirements laid down in Commission Implementing Regulation (EU) 2015/1998, the competent customs authority shall immediately make available to the appropriate national authority responsible for civil aviation security the following minimum information related to the AEO status which it has at its disposal:*

- (a) *the AEO authorisation, including the name of the holder of the authorisation and, where applicable, its amendment or revocation or the suspension of the status of authorised economic operator and the reasons therefor;*

- (b) *information about whether the specific site concerned has been visited by customs authorities, the date of the last visit, and whether the visit took place with a view to the authorisation process, re-assessment or monitoring;*
- (c) *any re-assessments of the AEO authorisation and the results thereof.*

*The national customs authorities shall, in agreement with the appropriate national authority responsible for civil aviation security, establish detailed modalities for the exchange of any information which is not covered by the electronic system referred to in Article 30.*

*The national authorities responsible for civil aviation security handling the information concerned shall use it only for the purposes of the relevant programmes for regulated agent or known consignor and shall implement appropriate technical and organisational measures to ensure the security of the information".*

Although the legislation does not require a specific form for establishing the monitoring system in general, the most appropriate way is that the competent customs authority draws up a monitoring plan. This plan may summarise all the findings of each audit and, if necessary, suggest corrective actions (even if the operator remains free to find a different solution than the suggested measure).

The monitoring of AEO operators by the competent customs authority may consist of:

- ensuring that the corrective actions are effectively implemented by the AEO;
- a follow-up of the operations of the AEO, to follow-up on existing risks and to prevent the emergence of new risks.

Regardless of the way customs authorities decide to organise the monitoring i.e. as a separate plan or part of the final report, the following shall be taken into account:

**-results of the audit** – monitoring should be primarily based on the AEO risk profiles as assessed by auditors during the performed auditing activities including any measures recommended to be taken by the AEO;

**- use of Article 28 (2) and/or (3) UCC IA relating to holders of a security and safety certificate issued on the basis of an international convention or of an International Standard of the International Organisation for Standardisation, or of a European Standard of a European standardisation body and regulated agents or known consignors** – these are important situations to be taken into account as in these cases the other relevant authorisation or certification granted by other government authorities have been used when granting the AEO status (e.g. RA, KC, etc.);

**- early warning signals** – as mentioned above the AEO is legally obliged to inform the competent customs authority of any significant changes. It is possible that the changes made by the AEO lead customs authorities to decide on the necessity for re-assessment. It is important that the AEO has a clear understanding of his or her obligations and the way to communicate any changes to the competent customs authority.

It is necessary that customs authorities have the possibility to continuously check thoroughly that the operator is still in control of its business and any risks identified or any changes in the situation (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 audit?). There are various ways allowing customs authorities to have early indications of any new risks/information, i.e.:

- random checking of declarations of the AEO;
- any physical inspections of goods undertaken;
- analysis of information available in internal customs databases;
- any audits other than AEO monitoring or re-assessment audits (i.e. audit under a simplified procedures or an application for authorised warehouse keeper status);
- evaluation of any changes in company's behaviour or trade patterns that come to notice.

**- monitoring of risks** - new risks or new situations must be assessed through monitoring. If one of the elements of the evaluation leads to the conclusion that the operator is not or no longer adequately addressing identified risks, the customs authority informs the operator about that conclusion. The operator then should undertake improvement actions. It is again the obligation of the customs authority to assess these improvement actions. This can also lead to the conclusion that re-assessment of one or more of the criteria and conditions should be done, or that the AEO status should be suspended or revoked immediately.

The monitoring activities to be planned should be based on risk analysis performed at the various stages (examinations before granting the status, management of the authorisation granted, etc.). There are a number of factors which can influence them:

- the type of authorisation held – while monitoring of some criteria, such as proven solvency, can be desk-based, monitoring of the security and safety criterion for AEOS should usually require an on-site visit;
- the stability of the economic operator – whether there are frequent changes to locations, markets, key personnel, systems etc.;
- the size of the business and number of locations;
- the role of the AEO within the supply chain – whether the AEO has physical access to goods or acts as a customs agent;
- the strength of internal controls over the business processes and whether processes are outsourced;
- whether any follow up actions or minor improvements to processes or procedures have been recommended during the AEO audit.

Consequently, the frequency and nature of monitoring activities varies depending on the AEO concerned and its related risks. However, considering the specific nature of the security and safety criterion, an on-site visit for AEOS is recommended at least once every 3 years.

Special attention shall be also given to the cases where the economic operator being granted the status of an AEO has been established for less than three years. In the latter cases customs authorities are required to carry out close monitoring during the first year after granting the AEO status.

It is also important to be taken into account that the development of the monitoring plan and in particular any visits in the premises of the AEO have to be done in the context of its overall

customs activities. Customs authorities should co-ordinate and take into account any other auditing/monitoring activities envisaged for that particular economic operator. Duplication of examinations has to be avoided as much as possible.

For the cases where Article 28 (2) and/or (3) UCC IA has been applied, any information available from other government authorities can be also used when planning any monitoring activities with regard to avoiding duplication of examinations both for customs authorities and economic operators.

The monitoring activities could result in specific actions of the competent customs authority. These specific actions shall be documented. The documentation can take, for instance, the following forms:

- an update of the monitoring plan,
- a lightened audit report,
- general conclusions and findings of the audit team etc.

This documentation shall indicate the criteria that have been checked and the results of these checks.

### **5.I.2. AEO authorisation covering several PBEs**

The general principles for monitoring as described in point 5.I.1 always apply. Nevertheless, in the cases of AEO status granted to a parent company for several PBEs, additional specific elements have to be taken into account. The general principle that the ICA is competent for granting the AEO status and has the leading role in the process shall be kept also for the phase of management of the issued authorisation. However, in these specific cases it has to be also considered that the 'practical' knowledge and information for a particular branch is with the customs authorities of the Member State where it is situated. Having this in mind and in order to have an efficient management of the authorisation when any monitoring activities are developed, the close cooperation between the competent customs authority and the customs authorities of the Member States where the separate PBEs are situated is of significant importance, as foreseen in Article 35 UCC IA. When elaborating the monitoring plan the following should be taken into account:

- it is recommended that one single general monitoring plan is developed for the AEO on whose name the status is granted. However it shall be based on the individual plans and information prepared by the Member State concerned;
- the ICA is responsible for the general coordination and framework of the plan, i.e. ensuring avoidance of any possible overlaps or duplication of control activities envisaged/done; gathering all new information and update of the plans etc.;
- customs authorities of Member States where the PBEs are situated are in general responsible for preparing the part of the monitoring plan related to the specific PBE. It has to be communicated to the ICA within a reasonable time-limit allowing it to prepare and coordinate the general monitoring plan. They are also responsible for any on-site visits to be done in the PBE.
- relevant information communicated by the AEO to any customs authority and relayed to the ICA.
- relevant findings made by a Customs authority in a PBE and shared with the ICA.

## **Section II – Re-assessment**

Article 15 (1) UCC DA requires that customs authorities re-assess whether an AEO authorisation holder continues to comply with the conditions and criteria of AEO where there are:

- "- where there are changes to the relevant Union legislation affecting the decision;*
- where necessary as a result of the monitoring carried out;*
- where necessary due to information provided by the holder of the decision in accordance with Article 23 (2) of the Code or by other authorities."*

Depending on the reason for the re-assessment, it can result in a full or partial re-examination of concrete criteria or conditions.

### **5.II.1. Re-assessment following changes to the EU legislation**

A re-assessment shall be required if there are changes in the Union customs legislation specific to and having impact on the conditions and criteria related to the AEO status. An example will be changes to the AEO criteria following modification of the Union Customs Code and its implementing provisions such as the new criterion on professional practical standards of competence or professional qualifications. Usually the legislation requires the re-assessment to be carried out within a specified transitional period.

### **5.II.2. Re-assessment following the result of a monitoring carried out or due to information provided by the holder of the decision or by other authorities**

The starting point for taking a decision for re-assessment is that there is reasonable indication that the criteria are no longer met by the AEO. This indication may arise from different situations – as a result of the monitoring that the customs authorities carried out; result of other checks carried out by customs or other government authorities; other information received from other customs or other government authorities; major changes in the activity of the AEO etc. It is up to the ICA to decide in each particular case whether re-assessment of all the conditions and criteria is necessary or if only the relevant condition or criteria for which there is indication for non-compliance are to be reassessed. It is always possible to discover even during the re-assessment of one of the criteria that the others should be also checked again.

The re-assessment shall be made by the ICA. However, any customs authority in another Member State may find out a reasonable indication that some of the criteria are no longer met by the AEO. This can occur, for example if:

- one or more of the AEO premises are located in a Member State different from the one of the ICA;
- the AEO carries out its customs related activities not only in the Member State where the AEO authorisation was issued.

In these cases, the customs authority of the Member State where this indication has emerged should inform the ICA about the facts, who decides whether to start a re-assessment and which other customs authorities are to be involved.

In the cases of an authorisation issued to the parent company for several PBEs, each of the Member States where the separate PBEs are situated can ask the ICA to start a re-assessment of the conditions and criteria.



In case the parent company establishes a new PBE or it goes through a restructuring process which has an impact on the PBE, it shall inform the ICA who takes the necessary measures including a re-assessment, if necessary.

Although in general the re-assessment to be done may vary from case to case, the following common elements should be taken into account:

- (a) **scope of the re-assessment** – the criteria and conditions to be checked or verified taking into account the reasons for starting the re-assessment.
- (b) **method of re-assessment** - only documentary check or combined with an on-site visit where appropriate for the specific criteria to be re-assessed;
- (c) **time-limit** – there is no time-limit specified for conducting a re-assessment. However, it has to be defined depending on the number of the criteria to be checked, whether an on-site visit is envisaged and normally it should not go beyond the same time-limits for the original AEO decision;
- (d) **re-assessments involving other Member States**- where the re-assessment involves a re-assessment of the criteria in other Member States, the rules for the consultation procedures in Part 4 'Exchange of information between Member States and with other government authorities' of these Guidelines shall apply. Normally, the customs authority in the other Member State will determine whether a visit is required as part of the re-assessment process. The time-limits for the other Member State(s) to respond should follow the normal time-limits for consultation under Article 31 UCC IA.
- (e) **other customs authorisations affected** - when a re-assessment is carried out, it is advisable to establish whether the AEO holds other authorisations or simplifications that are conditional on compliance with the AEO criteria, for example authorisation to use simplified procedures. Where this is the case, it should be taken into account and any possible duplication of re-assessment work both in terms of the customs resources and the economic operator concerned should be avoided.
- (f) **re-assessment report** - in terms of reports and documentation similar approach as for the original audit should apply. It is important that the subsequent action proposed is reflected in the report i.e. suspension, revocation, measures to be taken and deadlines.
- (g) **availability of the results** - it is necessary to make the results of the re-assessment available to the customs authorities of all Member States, and where appropriate other government authorities, using the communication system EOS no matter whether it has been involved in a consultation procedure or not.

### **Section III – Amendment of the decision**

In line with Article 28 UCC an AEO authorisation shall be revoked or amended in case one or more of the conditions for taking that decision were not or are no longer fulfilled or upon application by the AEO.

Revocation in the context of AEO is addressed in detail under 5.V of these Guidelines.

In the context of AEO possible examples for amendments are changes in name or address. In some cases these amendments can only take place after re-evaluation of the fulfilment of the criteria (e.g. new premises in case of an AEOS).

The amendment is to be notified to the AEO (Article 28 (3) UCC). Any amendment should be communicated to the customs authorities of all Member States, and where appropriate to other government authorities, using the communication system EOS, no matter whether it has been involved in a consultation procedure or not.

In addition, it is to be noted that the applicant has to communicate any changes relating to the application to the ICA who must upload these changes in the EOS system.

#### **Section IV - Suspension**

Suspension of the AEO status means that a granted authorisation is not valid during a specific period.

According to Article 23 (4) (b) UCC in conjunction with Article 16 UCC DA "*the customs authority competent to take the decision shall suspend the decision instead of annulling, revoking or amending where:*

- a. that customs authority considers that there may be sufficient grounds for annulling, revoking or amending the decision, but does not yet have all necessary elements to decide on the annulment, revocation or amendment;*
- b. that customs authority considers that the conditions for the decision are not fulfilled or that the holder of the decision does not comply with the obligations imposed under that decision, and it is appropriate to allow the holder of the decision time to take measures to ensure the fulfilment of the conditions or the compliance with the obligations;*
- c. the holder of the decision requests such suspension because he or she is temporarily unable to fulfil the conditions laid down for the decision or to comply with the obligations imposed under that decision.*

*In cases referred to in points (b) and (c), the holder of the decision shall notify the customs authority competent to take the decision of the measures he or she will take to ensure the fulfilment of the conditions or compliance with the obligations, as well as the period of time he or she needs to take those measures".*

*During the period of the suspension the AEO must not have access to the benefits that the status provides which can have serious consequences to him.*

Article 30 (1) UCC DA lays down that "*where an AEO authorisation is suspended due to the non-compliance with any of the AEO criteria, any decision taken with regard to that AEO which is based on the AEO authorisation in general or on any of the specific criteria which led to the suspension of the AEO authorisation, the customs authority having taken that decision shall suspend it".*

Article 30 (2) UCC DA lays down that "*the suspension of a decision relating to the application of the customs legislation taken with regard to an AEO shall not lead to the automatic suspension of the AEO authorisation".*

Article 30 (3) UCC DA lays down that "*where a decision relating to a person who is both an AEOS and an AEOC is suspended due to non-fulfilment of the conditions laid down in Article*

*39(d) UCC (practical standards of competence or professional qualifications directly relating to the activity carried out), his or her AEOC authorisation shall be suspended, but his or her AEOS authorisation shall remain valid".*

Where a decision relating to a person who is both an AEOS and an AEOC is suspended due to non-fulfilment of the conditions laid down in Article 39(e) UCC (appropriate security and safety standards), his or her AEOS authorisation shall be suspended, but his or her AEOC authorisation shall remain valid.

Suspension can be a potential consequence of an examination done during the monitoring or re-assessment where serious deficiencies have been discovered which means that the holder of the authorisation, from a risk perspective, cannot have the status under the present circumstances. This indication of 'non-compliance' may arise also as a result of information received from other Member States or other government authorities, e.g. civil aviation authorities.

Prior to the decision to suspend, the competent customs authority must notify the AEO of the findings, the assessments made and the fact that according to the evaluation they may result in a suspension of the authorisation if the situation is not corrected. The AEO is given the right to be heard and possibly to correct the situation. The timescale for comments and corrections is 30 calendar days from the date of communication (Article 8 (1) UCC DA).

The replies should be carefully assessed from a risk perspective and unless the situation can be regarded as corrected, the status will be suspended for 30 calendar days. The AEO must be notified in writing.

According to Article 22 (6) (c) UCC the status can be suspended with immediate effect if the type or extent of the threat to public safety and protection, public health or the environment requires such a decision. This possibility should be used restrictively.

In case the initiative for suspension of the status comes from the holder of the authorisation who is temporarily unable to meet any of the AEO criteria, the AEO should present the reason for the request and where appropriate, propose an action plan showing the measures to be taken and the expected time framework. For example an operator is optimising or changing its *computer*-integrated manufacturing and, for a while, he or she is not able to follow the goods in the international supply chain. He or she would ask for a suspension and propose a timetable for implementation.

The status can be suspended if the action plan and the reason for the requested service can be considered as reasonable. If not, a revocation of the authorisation on the demand of the holder should be discussed as a possibility.

However, it has to be taken into account that the distinction between suspension on the initiative of the customs authority and on the initiative of the AEO is very important and is clearly stated in the legislation (Article 16 (1) UCC DA). So, it cannot be used deliberately by AEO solely for the purpose to postpone revocation or avoid the three years period from the day of revocation, permitting the submission of a new application.

The competent customs authority should assess the effect of the suspension very carefully. The suspension will not affect a customs procedure which has been started before the date of the suspension and is still not completed.

When the reason to suspend is eliminated, the authorisation should be reinstated. If not, the competent customs authority has to consider whether the authorisation should be revoked.

## **Section V - Revocation**

The provisions on revocation of the authorisation and cases which could lead to the revocation are laid down in Articles 28 UCC and 34 UCC IA.

According to Article 28 (1) UCC a favourable decision shall be revoked where

- (a) *one or more of the conditions for taking the decision were or are no longer fulfilled; or*
- (b) *upon application by the holder of the decision.*

If a revocation is decided by the competent customs authority, a new application for an AEO authorisation will not be accepted within three years from the date of revocation.

The revocation of an AEO authorisation shall not affect any favourable decision which has been taken with regard to the same person unless AEO status was a condition for that favourable decision, or that decision was based on the AEO criterion which is no longer met (Article 34 (1) UCC IA).

The revocation or amendment of a favourable decision which has been taken with regard to the holder of the authorisation shall not automatically affect the AEO authorisation of that person (Article 34 (2) UCC IA).

Where the same person is both an AEOC and an AEOS, and the authorisation is revoked due to non-fulfilment of the conditions laid down in Article 39(d) of the Code (practical standards of competence or professional qualifications directly relating to the activity carried out), the AEOC authorisation shall be revoked and AEOS authorisation shall remain valid (Article 34 (3) first subparagraph UCC IA).

Where the same person is both an AEOS and an AEOC, and the authorisation is revoked due to non-fulfilment of the conditions laid down in Article 39(e) UCC (appropriate security and safety standards), the AEOS authorisation shall be revoked and AEOC authorisation shall remain valid (Article 34 (3) second subparagraph UCC IA).

It is to be noted that revocation on the initiative of the customs authorities is a customs decision and the economic operator has the right to be heard. Therefore, any findings, the assessment made and the fact that according to the evaluation this may result in revocation of the AEO status shall be notified to the AEO unless the right to be heard has been already expressed within the preceding suspension procedure. For any decision for revocation the economic operator has the right to appeal the decision.

## **PART 6, Mutual Recognition**

The following information focuses on the general background and process of Mutual recognitions Agreements and its implementation.

### **Section I - Mutual Recognition Agreements concluded by the EU**

Until now the EU has concluded and implemented Mutual Recognition of AEO programmes with Norway, Switzerland, Japan, Andorra, the US and China. Further negotiations are either already taking place or will be launched in the near future. In addition, the EU is providing technical assistance to a number of countries to prepare them to set up AEO programmes.

Details on the individual MRAs can be found on the DG TAXUD website under the following link:

[http://ec.europa.eu/taxation\\_customs/customs/policy\\_issues/customs\\_security/index\\_en.htm](http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/index_en.htm)

### **Section II - Process steps towards Mutual Recognition**

For the EU the following steps are necessary to achieve Mutual recognition

- Formal commitment to establish Mutual Recognition
- Comparison of legislation
- Assessment of implementation of the respective programmes and exchange of best practices including on-site visits on both sides (see [6.VII of these Guidelines](#) – recommendations on how to conduct monitoring/audit visits)  
Agreement on
- MRA text  
The MRA text would typically contain the following essential parts: It states the compatibility of the two AEO programmes, enumerates the reciprocal benefits to be granted, as precise as possible. It contains the data that is subject to the automatic data exchange and data protection rules. Furthermore it contains procedural rules, including rules on the unilateral suspension of benefits
- Electronic data exchange system

### **Section III - Implementation and follow-up after the signature of an MRA**

Due to the number of AEOs in the EU benefiting from Mutual Recognition and equally high numbers in the MRA partner countries, the development and deployment of an Automated Data exchange mechanism is essential for the implementation of an MRA. In other words, the implementation of an MRA can only start, once the automated data exchange mechanism is up and running.

Once an MRA has been concluded, the dialogue with the partner country continues. There are frequent exchanges of information, about recent developments, including cooperation in cases

of unilateral suspension of MRA benefits. Best practices regarding the implementation of an MRA include joint outreach to trade at conferences, seminars and the developments of joint Frequently Asked Questions (FAQs) that explain the technical aspects of the MRA.

The already available FAQs can be found on the DG TAXUD website under the following link:

[http://ec.europa.eu/taxation\\_customs/resources/documents/customs/policy\\_issues/customs\\_security/aeo\\_mra/2015-11\\_aeo\\_china\\_faqs.pdf](http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/aeo_mra/2015-11_aeo_china_faqs.pdf)

[http://ec.europa.eu/taxation\\_customs/resources/documents/customs/policy\\_issues/customs\\_security/aeo\\_mra/faq.pdf](http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/aeo_mra/faq.pdf)

In order to make sure that both sides keep their standards regarding the AEO procedures it is highly recommended that regular monitoring visits take place on both sides.

#### **Section IV - MRA Benefits proposed by the EU for members of partner AEO programmes (and reciprocal)**

The EU proposes the below mentioned MRA benefits to its MRA partners. Not all of those benefits are contained in current MR decisions; however the EU intends to update those decisions to include all those benefits. The concrete benefits are laid down in the individual agreements.

**(a) Fewer security and safety related controls:** each customs authority takes the status of a Programme Member authorised by the other customs authority favourably into account in its risk assessment to reduce inspections or controls and in other security and safety-related measures.

**(b) Recognition of business partners during the application process:** each customs authority takes the status of a Programme Member authorised by the other customs authority into account with a view to treating the Programme Member as secure and safe partner when assessing the business partners' requirements for applicants under its own Programme.

**(c) Priority treatment at customs clearance:** each customs authority takes the status of a Programme Member authorised by the other customs authority into account in ensuring priority treatment, expedited processing, simplified formalities and expedited release of the shipments where the Programme Member is involved.

**(d) Business continuity mechanism:** both parties endeavour to establish a joint business continuity mechanism to respond to disruptions in trade flows due to increases in security alert levels, border closures and/or natural disasters, hazardous emergencies or other major incidents, where priority cargos related to Programme Members could be facilitated and expedited to the extent possible by the customs authorities.

**(e) Future MRA benefits**

Customs administrations and trade are closely working together to identify and develop possible additional benefits for AEOs under Mutual Recognition to further enhance the programme.

## **Section V - Implementation of MRAs – How to benefit from MRAs?**

AEO companies with the security component that wish to benefit from the MRAs concluded by the EU need to check if they have provided their written **consent to the data exchange with MRA partner countries**. This written consent is requested in an [Annex to the SAQ](#) to be submitted together with the AEO application. In any case, this consent can be provided or withdrawn at any time by the applicant/AEO. In order to provide or withdraw the consent the AEO has to contact the ICA.

In order to benefit from the **“Recognition of business partners during the application process”** EU companies applying for AEO status in the EU may indicate the AEO number of any business partner they may have which is AEO in one of the countries that the EU has an MRA with (name, address, AEO number) in the [SAQ section 6.10](#). When a company applies for AEOS or AEOC/AEOS status in the EU and has business partners who are AEOs in one of the countries that the EU has an MRA with, these business partners are considered safe and secure and generally no additional requirements (security declaration etc.) will be asked from them.

In order to benefit from the **“fewer security and safety related controls and priority treatment at customs clearance”** the AEO has to communicate its EORI number to his or her business partner in the respective MRA partner country. The business partner enters the EORI number in the declaration form for the import process into the MRA partner country. Further details are available in the FAQs referred to under [6.III of these Guidelines](#).

## **Section VI - Unilateral Suspension of Benefits**

Under an MRA it cannot be excluded that one of the partner countries discovers a case of security related incident in which AEO companies of the other party are involved (e.g. a seizure of narcotics from a container of an AEO company).

For these cases the respective MRA decisions contain the legal basis for both sides to suspend the benefits of the AEO companies involved (e.g. Section III paragraph 3 MRA EU-Japan).

In those cases the information exchange will be conducted between designated Commission (DG TAXUD) and MRA partner country contact points, and between EU Member States and Commission (DG TAXUD) based on the agreed information exchange mechanisms. It will be conducted by secure e-mail.

## **Section VII - Recommendations for conducting an AEO audit or monitoring visit in an EU Member State**

One of the essential parts of the MRA negotiation with partner countries, as well as part of the monitoring as part of the MRA implementation are AEO audit or monitoring on-site visits.

The aim of the on-site visit is to observe how the EU AEO programme is implemented in practice by the different EU Member States. Such visits occur as part of the MRA negotiations (phase 2) and as part of the MRA implementation once an MRA has entered into force.

In general the main interest is to confirm that the EU AEO legislation is implemented in a uniform manner by the EU Member States.

It consists of two parts, first an introduction to the national AEO organisation and structure and an overview about the company to be visited. The second part is the actual visit to the company.

### **Discussion on the implementation of the EU AEO programme at Member State level**

The main interest is to see how the AEO programme is implemented from an operational point of view at Member State level.

It should include a brief overview of the:

- Customs Administration in general
- AEO organisational structure, e.g. number of staff dedicated to EU AEO (full time and part time, training system, outreach to business community)
- Authorization procedure, including application and the self-assessment questionnaire, how security requirements are checked
- Monitoring and post-audit
- Cooperation with other EU Member states (during authorisation and monitoring)

### **Company visit**

The aim of the company visit is to observe Member States' AEO auditors carrying out an audit at an applicant's premises or a monitoring visit at an AEO company. Representatives of the MRA partner country, COM and EU Member States customs administrations will participate at the site visit as observers.

It is essential that the companies are informed about the purpose of the exercise and that they know that the aim is to confirm that the AEO implementation in the EU Member State visited is in line with the EU standards



The visit to the premises of the applicant/AEO company is usually structured in the following way:

- The visit should consist of a real-life audit, which in particular should be guided by the AEO auditors – not by the company:
- The company should be informed in advance of this visit and how it will be conducted:
- Auditors should undertake their normal tasks
- in case of an audit during an AEO application
- in case of a Monitoring visit (existing AEO authorisation) i.e. ask the questions about recent developments that have an impact on AEOs, ask the company to explain or demonstrate their security procedures);
- In case translation is necessary, time should be provided to translate the content of the questions of the auditors and answers of the company. The company should be informed about this approach beforehand;
- The observers (from the MRA partner country) can only get a snapshot of the EU AEO audit/monitoring process;
- The validation visit should conclude with recommendations to the applicant;
- The audit exercise should focus on the Security and Safety ([Section 2.V](#) of these Guidelines).

**PART 7, ANNEXES**

# Self-assessment questionnaire

## AEO Guidelines

**0.1** Please note, it is recommended that you read the European Commission's Authorised Economic Operator Guidelines (TAXUD/B2/047/2011-REV6) before applying for AEO This is available via the European Commission's Europa website.

**0.2** Which departments including management, have you involved in the process to prepare your company for the AEO application? Have you involved customs or third parties in the process (consultants etc.)?

<b>1.</b>	<b>Company information</b>
<b>1.1.</b>	<b>General company information</b>

**1.1.1.** Please state the name, address, date of establishment and legal form of the organisation of the applying company. Include the URL of your company's website if applicable.  
If your company is part of a group, please provide a brief description of the group and indicate if any other entities in the group:  
a) already have an AEO authorisation; or  
b) have applied for AEO status and are currently undergoing an AEO audit by a national customs authority.

If you are submitting an application covering Permanent Business Establishments (PBEs),, please indicate their full names, addresses and VAT identification numbers.

If the company is established for less than three years, please specify whether the reason is due to an internal reorganisation of a previously existing company (e.g. incorporation or sale of a business unit). In this case please give details regarding the reorganisation.

- 1.1.2.** Please give the following details (if they apply to the legal form of your company):  
a) Full details of the owners or main shareholders including percentage shareholding held  
b) Full details of the board members and/or managers  
c) Full details of advisory board if any and board of directors  
d) Full details of the person in charge of your company or exercising control over your company's management.  
Details should include full name and address, date of birth and National Identification Number (e.g. national ID Card number or National Insurance Number).
- 1.1.3.** Please give full details of the person in charge of your customs matters.  
Details should include full name and address, date of birth and National Identification Number (e.g. national ID Card number or National Insurance Number)
- 1.1.4.** Please describe briefly your commercial activity and state your role in the international supply chain (manufacturer of goods, importer, exporter, customs broker, carrier, freight forwarder, consolidator, terminal operator, warehouse keeper, etc.). If you have more than one position, include all.
- 1.1.5.** Please specify the locations involved in customs activities, list the addresses, the name, the telephone numbers and the email of contact points and give a brief description of the business conducted in the following (including other MS and third countries):  
a) the individual locations of your company as a legal entity (please indicate approximate number of employees in each department),  
b) the sites where a third party executes outsourced activities for your company
- 1.1.6.** Do you buy from/sell to businesses with which you are associated? Yes/No
- 1.1.7.** Describe the internal organisational structure of your company and the tasks/ responsibilities of each department.
- 1.1.8.** Please give the names of senior management (Directors, heads of departments, head of accounting, head of customs department etc.) of the company and briefly describe the stand-in rules.

How many people are employed by your enterprise?

Please indicate one of these options

1.1.9.

- Micro
- Small
- Medium
- Large

1.1.10.

- a) If you agree to the publication of the information in the AEO authorisation in the list of authorised economic operators on the TAXUD website, please give your consent in [Annex 1 to this SAQ](#)
- b) If you can give your consent to the exchange of the information in the AEO authorisation in order to ensure the implementation of international agreements with third countries on mutual recognition of the status of authorised economic operators and measures related to security, please fill in [Annex 1 to this SAQ](#).

1.2.

**Volume of business**

1.2.1.

- a) Give the annual turnover figure for the last three sets of completed annual accounts. If a new business, state N/A.
- b) Provide the annual net profit or loss figure for the last three sets of completed annual accounts. If a new business, state N/A.

1.2.2.

If you use storage facilities which are not owned by you, please indicate who you rent/lease the storage facilities from.

1.2.3. For each of the following give an estimate of the number and value of the declarations you have made in each of the last three years. If a new business, state N/A.

- Import
- Export/Re-export
- Special procedures

1.2.4. Please give an estimate of the amount paid in each of the last three years for the following:

- Customs duty
- Excise duty
- Import VAT

If you are a new business operating for less than three years, provide details from the period you are operating. If you are a completely new business, state N/A.

1.2.5.

a) Do you foresee any structural changes in your company in the next 2 years?. If yes, please describe briefly the changes.

b) Do you foresee any major changes in the supply chain your company is presently involved in, during the next 2 years?. If yes, please describe briefly the changes.

**1.3. Information and Statistics on customs matters**

1.3.1.

a) Do you perform customs formalities in your own name and for your own account?

b) Are you being represented by someone regarding customs formalities, if yes by whom and how (directly or indirectly)? Please include the name, address and EORI number of the representative.

c) Do you represent other persons in customs formalities? If yes, who and how (directly or indirectly)? (Name the most significant clients)

**1.3.2.**

- a) How, and by whom, is the tariff classification of goods decided?
- b) What quality assurance measures do you take to ensure that tariff classifications are correct (e.g. checks, plausibility checks, internal working instructions, regular training)?
- c) Do you keep notes on these quality assurance measures?
- d) Do you regularly monitor the effectiveness of your quality assurance measures?
- e) What resources do you use for tariff classification (e.g. database of standing data on goods)?

**1.3.3.**

- a) How and by whom is the customs value established?
- b) What quality assurance measures do you take to ensure that the customs value is correctly established (e.g. checks, plausibility checks, internal working instructions, regular training, other means)?
- c) Do you regularly monitor the effectiveness of your quality assurance measures?
- d) Do you keep notes on these quality assurance measures?

**1.3.4.**

- a) Give an overview of the preferential or non-preferential origin of the imported goods.
- b) What internal actions have you implemented to verify that the country of origin of the imported goods is declared correctly?
- c) Describe your approach in the issuing of proof of preferences and certificates of origin for exportation.

**1.3.5.**

Do you deal in goods subject to anti-dumping duties or countervailing duties?

If yes, provide details of the manufacturer(s) or countries outside the EU whose goods are subject to the above duties.

**2.**

**Compliance record**

*(Article 39 (a) UCC; Article 24 UCC IA; [AEO Guidelines Part 2, Section I](#))*

**2.1.**

- Have breaches of customs and taxation rules been detected within your company or by the customs and/or fiscal authorities in the last three years?
- If so, briefly describe the breaches.
- a) How did you notify breaches to the relevant governmental authorities?
  - b) What quality assurance measures were introduced to avoid such breaches in the future?
  - c) Do you keep notes on these quality assurance measures?

Has your company been condemned for any serious infringement of criminal laws related to your economic activity?  
If yes, describe the infringement and when it has been committed. Please also make reference to the sentence of the court.

2.2.

a) Do you plan to apply or have you already applied for any other customs authorisation? Yes/No  
If yes, please provide details

b) Have any applications for authorisations/certifications been refused, or existing authorisations been suspended or revoked because of breaches of customs rules in the last three years? Yes/No.  
If yes, how many times and what were the reasons?

<b>3.</b>	<b>Accounting and logistical system</b> <i>(Article 39 (b) UCC, Article 25 UCC IA; <a href="#">AEO Guidelines Part 2, Section II</a>)</i>
<b>3.1.</b>	<b>Audit trail</b>

3.1.1.

Does your accounting system facilitate a full audit trail of your customs activities or tax relevant movement of goods or accounting entries?  
If yes, please describe the essential features of this audit trail.

<b>3.2.</b>	<b>Accounting and logistical system</b>
-------------	---

3.2.1.

What computer system (hardware/software) do you use for your business in general, and for customs matters in particular? Are those two systems integrated?

Provide information on the following:

- separation of functions between development, testing and operation
- separation of functions between users



- access controls (which ones/to whom)
- traceability between business system and declaration system.

**3.2.2.**

Are your logistical systems capable of distinguishing between Union and non-Union goods and indicating their location? Yes/No  
If yes, give details.  
If you do not deal with non-Union goods, please indicate N/A.

**3.2.3.**

a) At what location are your computer activities undertaken?  
b) Have computer applications been outsourced? If yes, provide details (name address, vat no.) of company or companies where the applications are outsourced and how do you manage access controls for the outsourced applications?

**3.3.**

**Internal control system**

**3.3.1.**

Do you have in house guidelines for the internal control system in the accounts department, buying department, sales department, customs department, production, material- and merchandise management and logistics? Yes/No.  
If yes please describe them briefly and how they are updated.  
For example, actions like job instructions, employee training, instructions for checking faults and mechanism for proof-reading.

**3.3.2.**

Have your internal control processes been subject to any internal/external audit? Yes/No  
Does this include audit of your customs routines? Yes/No.  
If yes, please provide a copy of your most recent audit report.

**3.3.3.** Describe in brief the procedures for checking your computer files (standing data or master files)? How do these procedures cover the following risks from your perspective:

- a) Incorrect and/or incomplete recording of transactions in the accounting system.
- b) Use of incorrect permanent or out-of-date data such as number of articles and tariff codes.
- c) Inadequate control of the company processes within the applicant's business.

**3.4. Flow of goods**

**3.4.1.** Describe briefly the registration procedure (physically and in the records) for the flow of goods starting from their arrival, the storage up to manufacture and shipment. Who keeps records and where are they kept?

**3.4.2.** Briefly describe the procedures in place for checking stock levels, including the frequency of those checks and how are discrepancies handled (e.g. stocktaking and inventory)?

**3.5. Customs routines**

**3.5.1.** Do you have documented procedures for verifying the accuracy of customs declarations, including those submitted on your behalf by, e.g., a customs agent or a freight forwarder? Yes/No.

If yes please describe briefly the procedures.

If no, do you verify the accuracy of customs declaration? Yes/No. If Yes in what way?

**3.5.2.** a) Does your company have instructions or guidelines on the notification of irregularities to the competent authorities (e.g. suspicion of theft, burglary or smuggling in connection with customs-related goods)? Are these instructions documented (e.g. work instructions, manuals, other guidance documents)?

b) Over the last year, have you detected any irregularities (or presumed irregularities) and notified them to the competent authorities? Yes /No

**3.5.3.** Do you trade in goods that are subject to economic trade licences e.g. textiles, agricultural goods? Yes/No  
If yes, please describe briefly your procedures for administering the licences related to the import and/or export of such goods.

**3.5.4.** a) Are you dealing with goods subject to import and export licenses connected to prohibitions and restrictions?  
b) Are you dealing with goods subject to other import and export licenses?  
c) If yes, please specify which type of goods and if you have procedures in place for the handling those licenses.

**3.5.5.** Are you dealing with goods falling under the Dual Use Regulation (Council Regulation No 428/2009/EC)? Yes/No  
If yes, have you implemented an Internal Compliance Programme (ICP)? Yes/No.  
If yes please describe them briefly and how they are updated.

**3.6. Procedures for back-up, recovery and fall back and archiving**

**3.6.1.** Describe briefly your procedures for back-up, recovery, fall back, archiving and retrieval of your business records

**3.6.2.** How long is the data saved in the production system and how long is this data archived?

**3.6.3.** Does the company have a contingency plan for system disruption/failure? Yes/No

**3.7. Protection of computer systems**

**3.7.1.** a) Describe briefly the actions you have taken in order to protect your computer system from unauthorised intrusion (e.g. Firewall, antivirus- programme, password protection).  
b) Has any intrusion testing been carried out, and if so what were the results and were any corrective measures necessary and taken?  
c) Have you experienced any IT security incidents in the last year?

3.7.2. a) Describe briefly how access rights for the computer systems are issued.  
b) Who is responsible for the running and protection of the computer system?  
c) Do you have guidelines or internal instructions for IT security for your personnel?  
d) How do you monitor that IT security measures are followed inside your company?

3.7.3. a) Please provide details on where your main server is located?  
b) Give details of how your main server is secured.

**3.8. Documentation security**

3.8.1. Describe briefly what actions have been taken in order to protect (e.g. constricted access rights, creation of electronic backup) information/documents from unauthorised access, abuse, intended destruction and loss?

3.8.2. Have there been any cases of unauthorised access to documents in the last year, and if so what measures have been taken to prevent this from happening again?

3.8.3. Please briefly answer the following questions:  
a) Which categories of employees have access to detailed data about the flow of materials and goods?  
b) Which categories of employees are authorised to change this data?  
Are changes comprehensively documented?

3.8.4. Describe briefly what requirements regarding security & safety you require from your trade partners and other contact persons in order to avoid abuse of information (e.g. endangering of the supply chain through unauthorised transfer of shipping details)?

**4. Financial solvency**  
*(Article 39 (c) UCC, Article 26 UCC IA, [AEO Guidelines Part 2 Section III](#))*

4.1. Have any bankruptcy or insolvency proceedings been initiated in respect of your company's assets in the last three years? Yes/No. If Yes please provide details.

**4.2.** Has your company a consistently good financial standing within the meaning of Article 26 of the UCC IA, sufficient to meet its financial commitments, over the last 3 years? If yes, please provide evidence such as a letter from your auditors or an audited report, a copy of your finalised accounts (including your management accounts) - if your accounts have not been audited, - evidence from your bank or financial institution. If no, please supply full details.

**4.3.** If you are a newly established business provide all records and information in relation to your financial status e.g. latest cash flow, balance sheet and profit and loss forecasts, approved by the directors/partners/sole proprietor.

**4.4.** Is there anything you are aware of that could impact on your financial solvency in the foreseeable future? Yes/No. If yes, give details.

<b>5.</b>	<b>Practical standards of competence or professional qualifications</b> <i>(Article 39 (d) UCC, Article 27 UCC IA, <a href="#">AEO Guidelines Part 2 Section IV</a>)</i>
<b>5.1.</b>	<b>Practical standards of competence</b>

**5.1.1.** Do you or the person in charge of your customs matters have practical experience of a minimum of three years in customs matters? Yes/No  
If yes, please provide details proving this experience.

**5.1.2.** Do you or the person in charge of your customs matters comply with a quality standard concerning customs matters adopted by a European Standardisation body, when available? Yes/No  
If yes, please provide details on this quality standard.

**5.2** **Professional qualifications**

**5.2.1.** Have you or the person in charge of your customs matters successfully completed training covering customs legislation consistent with and relevant to the extent of your involvement in customs related activities, provided by any of the following  
(i) a customs authority of a Member State;  
(ii) an educational establishment recognised, for the purposes of providing such qualification, by the customs authorities or a body

	<p>of a Member State responsible for professional training;          (iii) a professional or trade association recognised by the customs authorities of a Member State or accredited in the Union, for the purposes of providing such qualification?          Yes/No          If yes, please provide details regarding the training you or the person in charge of your customs matters have successfully completed.</p>
--	--

<b>6.</b>	<b>Safety and security requirements</b> <i>(Article 39 (e) UCC, Article 28 UCC IA, <a href="#">AEO Guidelines Part 2 Section V</a>)</i>
<b>6.1.</b>	<b>General information on safety and security</b>
<b>6.1.1</b>	Please give the name and the position of the person competent for safety and security related questions.

**6.1.2.** a) Have you carried out a risk and threat assessment for your business? Yes/No  
 b) Is there a security plan in place for each site (where appropriate)? Yes/No  
 How often are those documents reviewed and updated?

**6.1.3.** Describe briefly what security risks (within the company or in your business dealings with customers, suppliers and external service providers) you have identified in relation to the AEO security criteria?

**6.1.4.** How are security measures implemented and coordinated in your company and who is responsible for them?

**6.1.5.** If you have several premises in your company, is the implementation of the security measures harmonised in all of these locations? Yes/No

**6.1.6.** a) Do you have any security instructions? How are they communicated to your staff and people visiting your company premises?  
 b) How are they documented (manual, work guidelines, information sheet, etc.)?

**6.1.7.** a) Have you had any security incidents over the last year? Yes/No.  
If yes, please give a brief description of the incidents and what measures you have introduced to prevent them from re-occurring?  
b) Do you keep records of security incidents and the measures taken? Yes/No

**6.1.8.** a) Have you already been certified/authorised/approved by another public agency or authority for (transport, civil aviation, etc.) security purposes? Yes/No.  
If yes, please provide a copy of the certificate/authorisation/approval and give details of the premises/sites, which are covered by the relevant certificate/authorisation/approval.  
b) Provide a list of any independently accredited standards/licences/authorisations to which you adhere and specify what control/audits these standards are subject to.  
c) Have you planned to apply or have you already applied for any other certification/authorisation/approval for security purposes (e.g. regulated agent, known consignor, etc.)? Yes/No  
If yes, please provide details.

**6.1.9.** Are there particular security and safety requirements for the goods you are importing/exporting?

**6.1.10.** a) Do you use the services of a security company? If so, which company do you use?  
b) Has this company made a threat assessment of your company? If so, describe briefly what security risks they have identified in relation to the AEO security criteria.

**6.1.11.** Do your customers or insurance company impose any safety and security requirements on you? Yes/No  
If yes, provide details.

<b>6.2.</b>	<b>Building security</b> (AEO Guidelines <a href="#">Part 2 Section V, Subsection 2</a> )
-------------	--

**6.2.1.** a) Give a brief description of how the external boundary of your company's premises is secured. How is compliance with these procedures checked?  
b) How, by whom and at what intervals are checks carried out on the fences and buildings? How are these checks and their results recorded?  
c) How are security incidents reported and dealt with?

6.2.2. a) What types of access are there to your business premises?  
b) How are these managed?  
c) Are access points restricted to time/day?

6.2.3. Are the premises adequately illuminated (e.g. continuous light, movement sensors, twilight switch)?

6.2.4. How is the administration of keys handled in your company (e.g. location, access, logging)?  
Does written documentation exist for this? Yes/No

6.2.5. a) Is the parking of private vehicles permitted on the premises?  
b) If yes, for which persons?  
c) Who gives the approval?  
d) Are the vehicles checked (at the entrance to the premises or at the car park entrance)?  
e) Do you have written instructions? Yes/No

**6.3. Access to premises**  
*(AEO Guidelines Part 2 Section V, Subsection 3)*

6.3.1. a) Describe briefly how the process of access to your premises (buildings, production areas, warehouses etc.) is regulated for staff, visitors, other persons, vehicles and goods?  
b) Who checks that the prescribed procedures are complied with?

6.3.2. a) Describe the procedures that are to be followed if an unauthorised person/vehicle is discovered on company premises (grounds or buildings)?  
b) How are these procedures communicated to the staff (e.g. action plan, manual, working guidelines, training)?

6.3.3. Present a site plan for each location of your company that is involved in customs related activities (e.g. layout plan, draft) from which the frontiers, access routes and the location of the buildings can be identified, if available.

6.3.4. If applicable provide details of any other companies that are co-located on the same premises.



**6.4. Cargo units (as containers, swap bodies, transport boxes)**  
*(AEO Guidelines Part 2 Section V, Subsection 4)*

6.4.1. Is access to cargo units subject to rules/restrictions? Yes/No  
If yes, how are such restrictions enforced?

6.4.2. Describe briefly what measures are in place to prevent unauthorised access to and tampering with cargo units (particularly in open storage areas) (e.g. constant supervision, training staff and making them aware of risks, seals, instructions on procedures to follow in the case of unauthorised entry)?

6.4.3. a) Do you use seals to prevent unauthorised tampering with goods? If you do, what kind? Do these seals satisfy any specific standards (e.g. ISO)?  
b) How do you ensure that goods are not tampered with if seals are not used?

6.4.4. What control measures do you use for checking cargo units (e.g. seven-point inspection process: front wall, left side, right side, floor, covering/roof, inside/outside of doors, outside/undercarriage)?

6.4.5. Please answer the following questions:  
a) Who is the owner/operator of the cargo units?  
b) Who maintains/repairs the cargo units?  
c) Are there regular maintenance plans?  
d) Are external maintenance works checked?

**6.5. Logistical processes**  
*(AEO Guidelines Part 2 Section V, Subsection 4)*

6.5.1. a) Which means of transport are normally used by your company?  
b) Does your company carry out all its own transport, or does it also use external service providers (e.g. freight forwarders/carriers)?  
c) How do you establish whether the freight forwarder/carrier meets the required security standards (e.g. by means of a security certificate, declarations or agreements)?  
d) Do you take other measures for outsourced transport activities with a view to meeting security standards?

If appropriate please outline the nature and scope of your measures in this respect.

**6.6. Incoming goods**  
*(AEO Guidelines Part 2 Section V, Subsection 4)*

**6.6.1.** a) Describe briefly the procedure for ensuring the security and safety of incoming goods?  
b) Describe briefly how the compliance with these procedures is checked?

**6.6.2.** Are your employees informed about security arrangements with suppliers, and how is compliance ensured?

**6.6.3.** a) Describe briefly how checks on the integrity of the seals on incoming goods are conducted?  
b) Are incoming goods sealed if appropriate? Yes/No  
c) Does your company deal with specific types of goods requiring specific security measures (e.g. air cargo/air mail)?  
If Yes, what routines/measures are in place?

**6.6.4.** Are the incoming goods marked and if yes, how?

**6.6.5.** Describe briefly the process for counting and weighing incoming goods?

**6.6.6.** Describe briefly how, when and by whom incoming goods are checked against the accompanying documents and entered in your records?

**6.6.7.** a) Are the sections responsible for the purchase of goods, the receipt of goods and general administration clearly separated?  
Yes/No  
b) Do integrated internal control mechanisms exist between the sections? Yes/No. If yes, how are they executed?

**6.7. Storage of goods**  
*(AEO Guidelines Part 2 Section V, Subsection 4)*

**6.7.1.** Please describe at which locations you have set aside areas for the storage of goods?

6.7.2.	a) Please describe briefly the routine for allocating a storage position for incoming goods. b) Do you have outdoor storage locations? Yes/No. If yes, please describe them briefly.
6.7.3.	Do you have documented procedures for stock-taking and dealing with irregularities detected during stock-taking? Yes/No If yes, please describe your arrangements in brief.
6.7.4.	Are goods of different risk levels stored separately? Yes/No a) Please describe the criteria for any separate storage (e.g. hazardous goods, high-value goods, chemicals, weapons, air cargo/air mail)? b) Please describe how you ensure that the goods are immediately recorded in the logistical accounts/stock records?
6.7.5.	a) Describe briefly how goods are protected against unauthorised access to the warehousing premises? b) Describe briefly how compliance with these procedures is checked?
6.7.6	If storage of goods is outsourced to a third party please describe briefly how and where the goods are stored and your control measures you use to supervise the handling of goods.
<b>6.8.</b>	<b>Production of goods</b> <i>(AEO Guidelines Part 2 Section V, Subsection 4)</i>
6.8.1.	a) Describe briefly what locations/areas are designated for the production of goods? b) If production is carried out by an external partner (e.g. job processing, drop shipments), describe briefly how the integrity of the goods is ensured (e.g. contractual agreements)?
6.8.2.	Are there any security measures protecting goods against unauthorised access to the production zone? Yes/No. If Yes, describe briefly what these measures are and whether they exist in written form. Describe briefly how compliance with these procedures is checked?
6.8.3.	Describe briefly the procedures for packing products and whether they exist in written form.
6.8.4.	If final product packaging is outsourced to a third party, describe briefly how the integrity of the goods is guaranteed?
<b>6.9.</b>	<b>Loading of goods</b> <i>(AEO Guidelines Part 2 Section V, Subsection 4)</i>

- 6.9.1. a) Describe briefly how loading of goods is managed in your company (e.g. allocation of responsibilities, checks on goods, and means of transport, recording of results, provision of information, etc.)?  
b) Are there any written instructions on how the process should be organised? Yes/No
- 6.9.2. a) Are outgoing goods or vehicles sealed? Yes/No?  
If yes, how, by whom and what sort of seals do you use?  
b) Are any seal numbers mentioned in the documents accompanying the goods? Yes/No  
c) How do you keep a record of your seals?
- 6.9.3. Describe briefly how compliance with customers' security requirements for loading is guaranteed?
- 6.9.4. Describe briefly the arrangements that are in place which ensure that goods to be loaded and the loading process itself are not left unsupervised
- 6.9.5. Are the outgoing goods checked for completeness (e.g. counted, weighed)? Yes/No  
If yes, how and by whom?
- 6.9.6. Describe briefly how, when and by whom departing goods are checked against orders and loading lists and recorded out of the stock records?
- 6.9.7. Describe briefly what control mechanisms you have in place for detecting irregularities concerning the loading of goods?
- 6.10. Security requirements for business partners**  
*(AEO Guidelines Part 2 Section V, Subsection 5)*
- 6.10.1. Describe briefly how your company verifies the identity of trade partners in order to secure the supply chain (information search before accepting orders or placing orders).

6.10.2. a) Which measures have you taken to confirm that your business partners ensure the security of their part of the international supply chain (e.g. security declarations, contractual requirements, trade partners with own AEO- status)?  
b) Describe briefly how compliance with these procedures is checked?

6.10.3. Over the last year, have you detected any breaches of the security agreements you have with partners? Yes/No.  
If Yes, what measures have you taken?

**6.11. Personnel security**  
*(AEO Guidelines Part 2 Section V, Subsection 6)*

6.11.1. a) Describe briefly how your employment policy deals with security and safety requirements? Who is responsible for this area?  
b) Are the security procedures recorded in writing? Yes/No.  
c) Describe briefly how compliance with these procedures is checked?

6.11.2. To what extent are the following types of employees subjected to security checks (e.g. police checks to confirm that he/she has no criminal record):  
a) new employees who will be working in security-sensitive fields  
b) existing employees who are to be transferred into security-sensitive fields.  
  
How is it ensured that when staffs leave, they no longer have any physical or electronic access to company premises or data?

6.11.3. Is security and safety training provided for employees? Yes/No. If Yes:  
a) What is the frequency of security and safety training?  
b) Do you have yearly refresher training? Yes/No.  
c) Is this training internal or provided by an external supplier?  
d) Are there written records on this training? Yes/No.

6.11.4. Please answer the following questions:  
a) Specify the areas where temporary employees are used?  
b) Are these employees checked regularly according to security standards?  
If yes, how and by whom?  
Are there also security instructions for these employees?

6.12.

**External Services**

*(AEO Guidelines Part 2 Section V, Subsection 7; Annex 2 to the AEO Guidelines, point 4.12)*

6.12.1.

Do you use any “external services” under contract, such as transportation, security guards, cleaning, supplies, maintenance etc.?

Yes/No. If Yes:

a) Describe briefly what services they provide and to what extent (for the ones that have not been described in the previous sections).

b) Are there written agreements with the external service providers containing security requirements? Yes/No.

c) Describe briefly how compliance with the procedures included in these agreements is checked?

**Consent to disclose the AEO details on the TAXUD website**

I hereby give my consent to the publication of the information in the AEO authorisation in the list of authorised economic operators.

Signature.....

Capacity of Signatory.....

(The completed questionnaire should be signed by a Director/Managing Partner/Sole Proprietor as appropriate but for this case it is recommended that consent is given by an authorised signatory)

Date:.....

**Consent to the exchange of the information in the AEO authorisation in order to ensure the implementation of international agreements with third countries on mutual recognition of the status of authorised economic operators and measures related to security**

I hereby give my consent to the exchange of the information in the AEO authorisation in order to ensure the implementation of international agreements with third countries on mutual recognition of the status of authorised economic operators and measures related to security:

Signature.....

Capacity of Signatory.....

(The completed questionnaire should be signed by a Director/Managing Partner/Sole Proprietor as appropriate but for this case it is recommended that consent is given by an authorised signatory)

Date:.....

If you have provided your consent for mutual recognition please also provide the following information:

Transliterated name:.....

Transliterated street and number:.....

Transliterated postal code and city:.....

Only Latin characters should be used as codified in <http://www.unicode.org/charts/PDF/U0000.pdf>

## Explanatory notes for AEO-Self-Assessment Questionnaire

The purpose of the [AEO SAQ](#) is to help you as the applicant to understand the requirements associated with obtaining AEO status and provide Customs with information about you and your business in addition to that provided in your application. The information provided in the AEO-[SAQ](#) by the economic operator can also be used in the process of granting other authorisations in which it is necessary to be compliant with some or all of the AEO criteria. These instructions provide you both guidance on how to answer the questions in the [SAQ](#) as well as information on the standards customs authorities expect you to achieve and demonstrate to them in order to obtain the AEO authorisation.

According to Article 26 (1) of the Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council with regard to detailed rules of specifying some of the provision of the Union Customs Code (UCC DA) in order to apply for the status of Authorised Economic Operator (AEO) the applicant shall submit a Self-Assessment Questionnaire ([SAQ](#)), which the customs authorities shall make available, together with the application.

1. This questionnaire is built on the provisions of the Union Customs Code (UCC) and its implementing provisions (Implementing and Delegated Acts) as well as the AEO Guidelines. It aims to simplify and speed up the AEO application process.

It also allows for the Customs administration to get a good overall picture of the applicant together with the application form and that will result in speeding up the authorisation process. Economic operators are therefore invited to fill in the questionnaire in a correct way and answer to all relevant questions for their business.

You can find additional information about AEO status on the [European Commission's Europa website](#) and your national Customs administration's website.

Please note that it is important to read the applicable legislation and the European Commission's AEO Guidelines carefully, before starting the application process.



2. The questionnaire shall be submitted together with the application for an AEO authorisation to the competent customs authority (the manner of submission will be dependent on the facilities that the relevant customs authority has in place).

It is recommended to contact the competent customs authority should you have any questions or require further information regarding the questionnaire or the application before submitting them.

3. The questionnaire contains the most important issues that can be of use for the customs authorities under each section. However, some issues do affect only certain actors in the international supply chain. This can also vary depending on the type of authorisation that your company applies for. You do not need to answer questions that are irrelevant for your business. Please answer these issues with “Not applicable” followed by a short comment on why it is not applicable. You can for example make a reference to the part of the international supply chain that you are involved in or the type of authorisation you are applying for. Please see the specific table in Annex 2 of these Explanatory Notes for references regarding which questions are relevant for different actors in the supply chain and depending on the type of authorisation requested.

If you already have customs simplifications or other customs authorisations that demonstrate that one or more AEO criteria are fulfilled, then it is sufficient to refer to those simplifications or authorisations.

If your company holds certificates, expert reports or any other conclusions from experts (for example economic reviews, international certificates etc.), please either provide them or make reference to them. For more references refer to the corresponding section in the AEO Guidelines, which covers the relevant criteria either completely or in parts and indicate this in your answer to the relevant question. Note that this is not absolutely necessary, but if you have any of them it could be useful information for customs authorities and could result in speeding up the process.

Please note that all the questions may not be necessary to answer in all MS. This can vary depending on whether the customs authorities in that MS already have access to the information or not (for example through different databases). This mainly concerns sections 2 (Compliance record), 4 (Financial solvency) and 5 (Practical standards of competence or professional qualifications) of the [SAQ](#). The competent customs authority in the MS where you are going to apply will advise you if this applies.

4. It should be noted that individual answers to questions are not considered in isolation, but as part of an overall assessment process in relation to the criterion concerned. One unsatisfactory answer to a single question may not lead to a refusal of the AEO status in case the criterion is shown to be fulfilled elsewhere in the process (in overall terms).

5. The conditions and criteria for an AEO authorisation are the same for all economic operators. However, customs authorities will take into account the size of the company (e.g. Small and Medium Sized Enterprises (SME)), legal status of company, structure, the key business partners and also the specific economic activity. This means that the implementation of measures in order to fulfil the criteria can vary from operator to operator depending on size for example, without challenging the compliance of the requirements.

6. An AEO authorisation is based on the same principles as other international standards and where internal quality assurance standards are being adhered to by the company. **You as applicant are responsible for having quality assured procedures** at your premises, for customs matters as well as security and safety (if applicable). At the site visits your company should show the customs authorities that you have adequate internal procedures in place, in order to manage your customs and/or security and safety matters and adequate internal controls in order to assure that those procedures work properly. **Internal policies and/or instructions should be documented either electronically available or on paper. They must be known and applied within the organisation, be available to all users and of course continuously updated.**

Therefore, the first step relates to your internal quality assurance standards. The answers in the questionnaire submitted together with the application should be a summary of the internal procedures and instructions you have in place in order to give the customs authorities an overall picture of your business. In order to reply to the questionnaire and to be prepared for the AEO audit process all the main departments of your business involved in the international supply chain such as customs, logistics, accounting, computing, purchasing, sales, security, quality departments will have to be involved in the process.

7. Internal company policies or instructions regarding customs matters and/or security and safety, could be referred to in your answers in the questionnaire. If you do so, please specify the name or number of the document and keep this ready for an on-site audit by the customs authorities. To speed up the process it might be also possible to submit the documents (the manner of submission will be dependent on the facilities that the relevant customs authority has in place) together with the questionnaire.

8. The completed questionnaire shall be made available to the competent customs authority together with the application in an electronic form (preferably) or in writing.

9. The information sent within the application process falls under the data security legislation and will be treated as confidential.

## **Section I - Company's information**

*(Article 38 of the UCC)*

This section is mainly to give the customs authority an overview on the company. The information requested can be given in a general way and serves as a snapshot of applicant's activities on the date of the application submission. If the requested information is already available to the competent customs authority then indicate this on the form or provide a reference to when the information was submitted.

### **Sub-section 1.1 General company information**

#### **1.1.1**

For questions (a) and (b), please indicate the authorisation and the application references (name and EORI number, issuing customs authority and registration number).

If so, indicate what you share with these companies, for example if you share computer system(s), or if you have common standard security measures or common documental procedures, share premises, etc.

#### **1.1.2**

For question (a), include only shareholders who are involved in the day to day working/decision making process of the company.

#### **1.1.3**

The person in charge of customs matters is the person inside the company or a contracted person dealing with the applicant's customs matters.

#### **1.1.4**

Provide the appropriate NACE Revision 2 code (statistical classification of economic activities) of your commercial activities. A definition of the international supply chain is provided in Part 1, Section II of the AEO Guidelines.

For assessing and indicating your role in the international supply chain, please use the following guidance<sup>21</sup>:

---

<sup>21</sup> Codes used from UN/EDIFACT Party function code qualifier

**a) manufacturer of goods (MF):** Party who manufactures goods.

This code should be used only if the economic operator manufactures the goods. It does not cover cases where the economic operator is only involved in trading with the goods (e.g. exporting, importing).

**b) importer (IM):** Party who makes, or on whose behalf a Customs clearing agent or other authorised person makes an import declaration. This may include a person who has possession of the goods or to whom the goods are consigned.

This code should be used only if the economic operator has the possession of the goods. In case of customs representatives/agents, please use the code for 'customs broker'.

**c) exporter (EX):** Party who makes, or on whose behalf the export declaration is made, and who is the owner of the goods or has similar rights of disposal over them at the time when the declaration is accepted.

In case of customs representatives/agents, please use the code for 'customs broker'.

**d) customs broker (CB):** Agent or representative or a professional Customs clearing agent who deals directly with Customs on behalf of the importer or exporter.

The code can be used also for economic operators who act as agents/representatives also for other purposes (e.g. carrier's agent)

**e) carrier (CA):** Party undertaking or arranging transport of goods between named points.

**f) freight forwarder (FW):** Party arranging forwarding of goods.

**g) consolidator (CS):** Party consolidating various consignments, payments etc.

**h) terminal operator (TR):** Party which handles the loading and unloading of marine vessels.

**i) warehouse keeper (WH):** Party taking responsibility for goods entered into a warehouse.

Warehouse should not be considered compulsory as customs warehouse; therefore this code should be used also by economic operators who are other storage facility operators (e.g. temporary storage, free zone, etc.).

**j) others:** e.g. container operator (CF), stevedore (DEP), shipping line service (HR).

In case you have more than one role in the international supply chain, please include the relevant codes to indicate them.

#### **1.1.5**

Provide details of the locations involved in customs activities (if you have more than five locations involved in customs activities, please provide only details of the five principal locations involved in customs activities) and addresses for the remaining locations involved in such activity.

In case of new locations involved in customs activities during the AEO application process, you must provide full details of them.

#### **1.1.6**

This is to determine whether you trade (goods, not services) with your associated businesses or not. For example, all your purchases are from your parent company in the USA or you import on behalf of and distribute to associated businesses in MS. You must provide full details during the authorisation process.

#### **1.1.7**

A detailed organisational chart including the different areas/departments of your business, their functions/responsibilities and the management chain may be provided in this respect.

#### **1.1.8**

Where not already mentioned in questions 1.1.2 (b) and (c), please indicate full name and address, date of birth and National Identification Number (e.g. national ID card number or National Insurance Number).

The procedures should outline the arrangements for dealing with temporary or short term absences of key staff e.g. customs manager, import clerk including how their normal responsibilities are covered and by whom.

#### **1.1.9**

Provide the (approximate) number known at the time of submission of your application. In this context please indicate if your company falls within the definition of micro, small and medium-sized enterprises as defined the Commission Recommendation of 6 May 2003 OJ L 124/2003. The table below is based on the above mentioned recommendation:

Company category	Staff headcount	Turnover	or	Balance sheet total
Large	$\geq 250$	any		any
Medium-sized	$< 250$	$\leq \text{€ } 50 \text{ m}$		$\leq \text{€ } 43 \text{ m}$
Small	$< 50$	$\leq \text{€ } 10 \text{ m}$		$\leq \text{€ } 10 \text{ m}$
Micro	$< 10$	$\leq \text{€ } 2 \text{ m}$		$\leq \text{€ } 2 \text{ m}$

### **Sub-section 1.2 Volume of business**

#### **1.2.1**

If you are a new business and have fewer than three full sets of accounts, provide details from those which have been completed. If you have not traded long enough to have produced any finalised full sets of accounts, state “not applicable”.

#### **1.2.2**

Please indicate the location of the storage facilities used, but not owned by you (if you have more than five sites indicate the 5 main facilities and the total number of facilities and all facilities located in other MS).

#### **1.2.3**

For customs agents/third party representatives, include all declarations made both in your name and on behalf of others.

An example:

	Import	Export	Special Procedures (differentiated between transit, storage, specific use, processing)
--	--------	--------	---

	number	value	number	value	number	value
2013	2200	€9.6 m	400	€2.6 m	150	€0.8 m
2014	2500	€10.3 m	350	€2.2 m	100	€0.4 m
2015	2400	€10.2 m	340	€2.1 m	100	€0.5 m

#### 1.2.4

For customs agents/third party representatives, include all revenue paid through your customers' or your payment facilities.

An example:

	Customs duty	Excise duty	VAT
	€300 m	€1.75m	€2.32m
	€400m	€1.87m	€2.12m
	€380m	€1.85m	€2.10m

#### 1.2.5

Known future changes are the changes which may influence the organisation of the company, the fulfilment of the AEO criteria or the risk assessment of the international supply chain. This may include for example changes in key personnel, changes to your accounting system, opening new sites, awarding new logistics contracts etc.

Sub-section 1.3 Information and statistics

#### 1.3.1

For questions (b) and (c), if your partner(s) are currently undergoing an AEO audit, please indicate the authorisation and/or the application references (name and EORI number, issuing customs authority and registration number).

### **1.3.2**

For question (a), please indicate the name and position of the member of staff responsible for classifying your goods or if you use a third party to do this work, include their name.

For questions (b) and (d), especially if you use a third party, how do you ensure that this work has been done correctly and according to your instruction?

For question (b), indicate whether you maintain a product file in which each article is linked to a commodity code with the appropriate duty and VAT rates.

For question (c), if quality assurance measures are put in place, you should provide evidence, during the visit of customs auditors, that you regularly and fully review them, document any changes and notify affected staff of the changes.

For question (d), please indicate how, by whom and how often you review the classifications and update the product file and any other dependant records as well as notify any persons affected by the change e.g. customs agent, purchasing staff.

For question (e), indicate also if you use any Binding Tariff Information(s) BTIs.

Please be prepared that during the audit process you might need to make available:

- details/lists or product files of your products and their relevant commodity codes and duty rates;
- the resources/information, e.g. up to date tariff, technical information, that you usually use to classify your goods.

### **1.3.3**

(a) Indicate the name and position of the member of staff responsible for the valuation of goods or in case you use a third party to do this work, include their name.

(b) and (d) - If you use a third party, how do you ensure that this work has been done correctly and according to your instruction?



- (b) The quality assurance measures should include, for instance,
- the evaluation method(s) used,
  - how valuation statements are completed and submitted when required,
  - how the customs and VAT values are determined,
  - how freight and insurance costs are accounted for,
  - royalties and licence 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 is paid 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
  - costs incurred in relation to containers and packaging, goods and/or services supplied by the buyer free of charge or at reduced cost for use in connection with the production and sale for export of the imported goods.
- (c) If quality assurance procedures are put in place, during the visit of customs auditors you should provide evidence that you regularly and fully review your procedures, document any changes and notify affected staff of the changes.

#### **1.3.4**

For question (b), internal actions would normally include measures on how you ensure that:

- the exporting country is entitled to give a preference and that the goods attract a preferential rate of duty;
- the direct transport/non-manipulation requirements are met;
- a valid and original certificate or an invoice declaration is available when preference is claimed;
- the certificate or invoice declaration is appropriate for the consignment and that the origin rules are met;
- there is no opportunity to duplicate use of the certificate/invoice declaration
- import preferences are claimed within the period of validity of the certificate/invoice declaration, and
- the original certificates/invoice declarations are retained as part of the audit trail in a safe and secure manner

For question (c), your approach should consider the way to ensure that:

- goods qualify for an export preference, e.g. meet the rules of origin;
- all necessary documents/calculations/costing/descriptions of processes to support preferential origin and the issue of a certificate/invoice declaration are retained as part of the audit trail in a safe and secure manner;
- appropriate documents e.g. certificate or invoice declaration are signed and issued timely by an authorised member of staff;
- invoice declarations are not issued for medium and high value consignments unless you have been approved by customs to do so;
- unused certificates are stored safely and securely, and
- certificates are presented as required to customs at export.

### 1.3.5

Provide as appropriate:

- the names of the non-EU countries and/or
- the names and addresses of the manufacturers on whose goods you have to pay anti-dumping or countervailing duties.

## **Section II - Compliance record**

*(Article 39 (a) of the UCC, Article 24 of the UCC IA22; [AEO Guidelines Part 2, Section I](#); [Annex 2 to the AEO Guidelines point 1](#))*

***NB: Pursuant to Article 24 of the UCC IA, the record of compliance with customs legislation and taxation rules of your company and the persons identified in questions 1.1.2, 1.1.3 and 1.1.8 will be based on the last 3 years preceding the application. During that time you should not have committed a serious infringement or repeated infringements of customs legislation and taxation rules. However,***

---

<sup>22</sup> COMMISSION IMPLEMENTING REGULATION (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code

*the record of compliance may be considered as acceptable if the infringements are of minor importance in relation to the number or size of the related operations/activities and do not create doubts concerning the overall compliance levels.*

*In doing so, customs will consider:*

*irregularities/errors as a whole and on a cumulative basis*

- *their frequency to establish if there is a systematic problem*
- *if there was any fraudulent intent or negligence*
- *whether you notified Customs voluntarily of the error/irregularities you discovered*
- *if you took any remedial action to prevent or minimise future errors.*

*Article 24 UCC IA also requires that the person identified in questions 1.1.2, 1.1.3 and 1.1.8 have had no records of serious criminal offences relating to its economic activity.*

#### **2.1 a)**

Examples of breaches of customs rules detected:

- March to September 2015 – use of incorrect currency code on imports from China resulting in an over declaration of customs duty and VAT of €5500.
- December 2015 – quarterly Inward Processing Regime suspension return not submitted.

Examples of breaches of taxation rules detected:

- January 2016 – illegal manufacturing or refining of mineral oil and subtraction.

If there are several, provide a total number and a brief summary of the main reasons for the errors.

#### **2.1 b)**

Examples of quality assurance measures taken as a result of the 2 instances at 2.1a) above:

- 6.10.2015 - computer system change to prevent entries being finalised until check performed on declared currency.
- outstanding return submitted. Inward Processing Regime suspension return procedures reviewed to include quarterly management checks and issued to relevant staff.

Your quality assurance measures would normally include:

- the appointment of a responsible contact person within your business to disclose irregularities/errors, including suspicion of criminal activity, to Customs or other government departments;
- requirements, including frequency, for checks to be performed and evidenced on the accuracy, completeness and timeliness of the recording and maintenance of records e.g. declarations/returns made to customs and other regulatory authorities, compliance with the conditions of approvals/ authorisations;
- use of internal audit resources to test/gain assurance of your procedures;
- how staff are notified of requirements/changes;
- the frequency of future reviews;
- management checks to ensure procedures followed.

## 2.2

For example:

May 2015 – refusal of customs warehouse application due to lack of economic need.

June 2016 – withdrawal of Local Clearance Procedure authorisation due to persistent failure to submit supplementary declarations.

The refusal/suspension/withdrawal of any application/authorisation for customs decisions will not necessarily result in the rejection of your AEO application.

### **Section III - Accounting and logistical system**

*(Article 39 (b) of the UCC, Article 25 of the UCC IA; [AEO Guidelines Part 2, Section II](#); [Annex 2 to the AEO Guidelines point 2](#) )*

***In order to comply with the criterion mentioned in Article 25 (1) letter (a) to (d) of the UCC IA***, you must maintain an accounting system which allows audit-based customs control. To enable customs to apply the necessary controls, you must allow customs to have physical and – in case your systems and record are kept electronically - electronic access to your records.

**In order to comply with the criterion mentioned in Article 25 (1) letter (e) of the UCC IA**, you must also have a logistical system which distinguishes between Union and non-Union goods, and indicates, where appropriate, their location, though this condition is not appropriate in the case of an AEOS.

### **Sub-section 1: The audit trail**

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

The accounting system would normally include:

- general ledger
- sales ledger
- purchase ledger
- assets
- financial statements (balance sheet, income statement, statement of cash flows and statement of stockholders equity)
- management accounts

The logistical system would normally include:

- sales order processing
- purchase order processing
- manufacture
- inventory – storage, warehousing
- shipping/transport
- supplier/customer lists

### 3.1

Your audit trail should include:

- sales
- purchases and purchase orders
- inventory control
- storage (and movements between storage locations)
- manufacture
- sales and sales orders
- customs declarations and documentation
- shipping
- transportation
- accounting e.g. invoicing, credit and debit notes, remittances/payments

### Sub-section 3.2: The accounting and logistical systems

#### 3.2.1

Indicate if you use:

a) hardware such as:

- sole reliance on a free standing personal computer(PC),
- PCs which are networked together
- a “server” based computer system
- a mainframe based system
- other

b) software such as computer programmes which allow the computer to run and execute the software applications that support the business, e.g. Windows, UNIX, etc.

c) systems such as (provide the name of the supplier):

- a fully integrated ERP solution
- a combination of accounting and logistical software applications
- a business software solution focused on small and medium sized enterprises
- a software solution developed by or for your business.

***NB: during the authorisation process, you will need to demonstrate:***

- *the extent of the computerisation*
- *the hardware platform available and the operating system running on it*
- *the segregation of functions between development, testing and operations*
- *the segregation of functions amongst users*
- *how access to the various parts of the system is controlled*
- *whether there have been any adaptations to the standard package*
- *the list of ledger accounts*
- *whether the system makes use of verification interim accounts*
- *how liabilities to customs/excise duty/VAT are recoded in the ledger*
- *whether you operate in batches*
- *whether your stock and financial records are linked*
- *how you manage your records, where these are maintained by a third party software provider*

### **3.2.3**

In case the activities, for example setting up standing data or keying data, are split between more than one location, advise which activities are carried out at each location.

### **Sub-section 3.3 Internal control systems**

*As provided for in Article 25 (1) letter f of the UCC IA*, you should have an administrative organisation which corresponds to the type and size of your business and which is suitable for the management of the flow of goods, and have internal controls capable of preventing and detecting illegal or irregular transactions.

#### **3.3.1**

During the visit of auditors, you should provide evidence that you regularly and fully review your procedures, document any changes and notify affected staff of the changes.

#### **3.3.2**

Examples of the types of audit may be:

- internal audit within your company or by your parent company;
- external audit by customers, independent accountants/auditors, customs or other government departments.

You will also need to make any reports available when customs authorities visit your facilities as well as evidence of any remedial action taken to correct any deficiencies identified.

#### **3.3.3**

Standing data or master files mean key information about your business e.g. customers' names and addresses, suppliers, product files containing information on the description of the goods, commodity codes and origin etc.

### **Sub-section 3.4 Flow of goods**

#### **3.4.1**

Your registration procedures should include, before and during the arrival of goods:

- purchase ordering procedures
- confirmation of order
- shipping/transport of goods



- supporting documentation requirements
- transport of goods from the frontier to your or your customers' premises
- receipt of goods at your or customers' premises
- payment/settlement
- how, when and by whom are goods entered into the stock record,

During the storage of goods,

- a clear assignment of a location for storage of the goods
- safe storage of dangerous/hazardous goods
- whether stock is recorded by value and/or quantity
- existence and frequency of stock-taking
- if a 3<sup>rd</sup> party's premises is used to store your goods, arrangements including reconciliation between your and 3<sup>rd</sup> party's stock record
- if a temporary location is used to store the goods,

During the manufacturing process of goods,

- raising the works order
- requisitioning of stock items and delivery from storage
- manufacturing process, staff responsibilities, and records maintained
- recipe codes
- recording the manufactured product and unused stock in the stock records
- use of standard manufacturing methods in the production,

And during the shipping process of goods,

- receiving customer order and raising works or purchase order
- informing the warehouse of the sale order/release of the goods
- instructions to 3<sup>rd</sup> party if goods stored elsewhere
- picking
- packing procedures
- how, when and by whom are the stock records updated.

### 3.4.2

Your checking and quality control procedures should include, during the arrival of goods:

- reconciliation between purchase order and goods received
- arrangements for returning/rejecting goods
- arrangements for accounting and reporting short and over shipments
- arrangements for identifying and amending incorrect entries in the stock record
- identification of non-Community goods within the system,

During the storage of goods,

- recording and controlling the stock
- identifying Community and non-Community goods (not appropriate for a AEOS)
- movement and recording of goods between locations within the same premises or different sets of premises
- arrangements for dealing with breakages, deterioration or destruction of goods, losses and stock variations,

During the manufacturing process,

- monitoring and management controls of the manufacturing process e.g. rates of yield
- how you deal with irregularities, variations, waste, by-products and losses in the manufacturing process
- quality inspection of manufactured goods and recording of results
- safe disposal of hazardous goods,

And, during the shipping process of goods,

- despatch/collection notes
- transport of goods to your customers or to the frontier for (re-)export
- raising sales invoices
- instructions to agent for (re-)exports and raising/availability/control of supporting documents
- acknowledgement of receipt/evidence of shipment of goods
- returned goods – inspection, counting and recording in stock
- payment and credit notes
- dealing with irregularities, short shipments and variations.

### Sub-section 3.5 Customs routines

*In order to comply with the criterion mentioned in Article 25 (1) letter g of the UCC IA, you should where applicable, have satisfactory procedures in place for the handling of licenses and authorisations granted in accordance with commercial policy measures or relating to trade in agricultural products;*

*In order to comply with the criterion mentioned in Article 25 (1) letter i of the UCC IA, you should ensure that relevant employees are instructed to inform the customs authorities whenever compliance difficulties are discovered and establish procedures for informing the customs authorities of such difficulties.*

### **3.5.1**

As importers, exporters, warehouse keepers, your procedures should include:

- how you ensure the completeness, accuracy and timeliness of customs declarations you make yourself, including performing management checks;
- presentation or availability of supporting documentation;
- up to date details (names and addresses) of customs agents/third parties used;
- how customs agents are appointed e.g. the credibility and suitability checks you perform before you appoint them;
- the circumstances when they are used;
- contracts detailing responsibilities, including the type of representation by customs agent e.g. direct, indirect;
- the way you provide clear and unambiguous instructions to your customs agent;
- how you provide supporting documents (e.g. licences, certificates etc.) to your customs agent, including presentation and retention/return;
- what the customs agent should do if the instructions are unclear;
- checking/verification of the accuracy and timeliness of your customs agent's work by you;
- how you notify your customs agent of any errors/amendments regarding cleared entries;
- dealing with irregularities;
- voluntary disclosures of errors to customs.

As third party representatives, your procedures should include:

- contracts detailing responsibilities, including the type of representation to be used by you e.g. direct, indirect;

- how you ensure the completeness, accuracy and timeliness of customs declarations you make, including performing management checks;
- prompt presentation or availability of supporting documentation;
- how your staff are aware of customers' and contract requirements;
- what you do if the customers' instructions are unclear or the details provided are incorrect;
- what you do if you discover any errors/amendments regarding cleared entries;
- voluntary disclosures of errors to customs.

### **3.5.2**

Where these instructions are documented, you should provide evidence, during the visit of customs auditors, that you regularly and fully review them, document any changes and notify affected staff of the changes.

### **3.5.3**

If procedures for the handling of licenses and authorisations are in place, you should provide evidence, during the visit of customs auditors, that you regularly and fully review your procedures, document any changes and notify affected staff of the changes.

### **3.5.4**

In order to comply with the criterion mentioned in Article 25 (1) (k) UCC IA, where applicable, satisfactory procedures should be put in place for the handling of import and export licenses connected to prohibitions and restrictions (such as embargos, dangerous goods etc.), including measures to distinguish goods subject to the prohibitions or restrictions from other goods and measures to ensure compliance with those prohibitions and restrictions. For dual use goods, please see question 3.5.5.

### **3.5.5**

In case you are dealing with goods falling under the Dual Use Regulation (Council Regulation No 428/2009/EC), you should provide customs authorities with a list of these goods. You should also inform the customs authority if you have implemented an Internal Compliance Programme (ICP).

## **Sub-section 3.6 Procedures for back-up, recovery and fallback and archiving**

*In order to comply with the criterion mentioned in Article 25 (1) letter (h) of the UCC IA*, you should have satisfactory procedures in place for the archiving of your records and information and for protection against the loss of information.

### **3.6.1**

Your procedures should include on what kind of media the data is stored, in which software format the data is stored and whether the data gets compressed and at what stage. If a third party is used, please indicate the arrangements, the frequency and location of any back-up and archived information.

## **Sub-section 3.7 Protection of computer systems**

*In order to comply with the criterion mentioned in Article 25 (1) letter (j) of the UCC IA*, you should have appropriate security measures in place to protect your computer system from unauthorised intrusion and to secure your documentation.

### **3.7.1**

For question (a), your actions should consider:

- an updated safety plan describing the measures in place protecting your computer system from unauthorised access as well as deliberate destruction or loss of information;
- details of whether you operate multiple systems at multiple sites and how they are controlled;
- who is responsible for the protection and running of the company's computer system (responsibility should not be limited to one person only, but to several persons who are able to monitor each other's actions);
- details of firewalls, anti-virus and other malware protection;
- a business continuity/disaster recovery plan in case of incidents;
- back-up routines including restoration of all relevant programmes and data following the disruption due to a breakdown of the system;
- logs where each user and his actions are recorded;
- whether the vulnerability management of the system is done periodically and by whom.

For question (b), indicate the frequency of testing your system against unauthorised access, the recording of results, and how to deal with incidents when the system has been compromised.

### **3.7.2**

Your access rights procedures should include:

- how you issue authorisation for access and the level of access to the computer systems (access to sensitive information should be limited to staff who are authorised to apply changes/additions to the information);
- the format for setting passwords, frequency of changes and who issues passwords, and
- removal/maintenance/updating of user details.

### **Sub-section 3.8 Documentation security**

#### **3.8.1**

Your actions should normally include:

- recording and back-up of documents including scanning and microfiche, and limiting access;
- an updated safety plan describing the measures in place to protect documents from unauthorised access as well as their deliberate destruction or loss;
- the filing and safe, secure storage of documents including responsibilities for their handling;
- dealing with incidents which compromise document security.

#### **3.8.2**

Your measures should consider

- testing your system against unauthorised access and recording the results;
- business continuity/disaster recovery plan;
- documented remedial action taken as a result of any actual incidents.

### **Section IV- Financial solvency**

*(Article 39 (c) of the UCC, Article 26 of the UCC IA; [AEO Guidelines Part 2, section III](#); [Annex 2 to the AEO Guidelines point 3](#)).*

Solvency means a good financial standing which is sufficient to fulfil your commitments with due regard to the characteristics of your type of business activity and will be based on the last 3 years. If you have operated for less than 3 years, then your financial solvency will be judged on the basis of records and information that are available (see question 4.3). These records should only relate to the applicant

making the AEO application. Any known information that will affect your solvency in the foreseeable future should be given in question 4.4.

**4.1**

Please enter details of any insolvency, bankruptcy or liquidation proceedings taken against your company or company assets in the last three years.

**4.2**

The evidence or information required may concern also any contingent liabilities or provisions, the net current assets position or the net assets position and the extent of intangible assets.

In some circumstances 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 but customs authorities may require further evidence such as an undertaking from the lender, reference to the use of a guarantee from a parent company or a bank facilities letter to satisfy the requirement or, if you are a sole proprietor or partnership a list of any personal assets that are used to support the solvency of the business.

***NB: To determine your financial solvency customs may require the submission of your annual accounts to be up to date. Customs authorities may need to inspect copies of your full sets of annual accounts or statements for the last 3 years during their visit. Customs authorities may also ask to see the most recent management accounts to establish the most up to date financial situation.***

**Section V- Practical standards of competence or professional qualifications**

*(Article 39 (d) of the UCC, Article 27 of the UCC IA, [AEO Guidelines Part 2, Section IV](#))*

**Note:**

This section concerns the criterion on practical standards of competence or professional qualifications for AEO. It should **only** be completed if you are applying for an AEOC authorisation.

In order to comply with the criterion mentioned in Article 27 of the UCC IA, you or the person in charge of your customs matters must comply with one of the following practical standards of competence: a proven practical experience of a minimum of three years in customs matters or a quality standard concerning customs matters adopted by a European Standardisation body. Alternatively you or the person in charge of your customs matters must have successfully completed training covering customs legislation consistent with and relevant to the extent of your involvement in customs related activities, provided by any of the entities listed in Article 27 (1) letter (b) of the UCC IA.

The person in charge of customs matters in this context is the person referred to under [1.1.3 the SAQ](#) and its Explanatory Notes.

**5.1.1.**

Possible ways by which to prove the practical experience of a minimum of three years in customs matters are described in detail under 2.IV.2.1 of the AEO Guidelines.

**5.1.2.**

At the time of preparing these Explanatory Notes, the work on quality standards concerning customs matters adopted by a European Standardisation body is still ongoing.

**5.2.1.**

As regards the training covering customs legislation consistent with and relevant to the extent of your involvement in customs related activities, it is to be noted that not in all Member States a respective training might be offered. The economic operator can follow a training in any EU Member State.

**Section VI- Security and Safety requirements**

*(Article 39 (e) of the UCC, Article 28 of the UCC IA; [AEO Guidelines Part 2, Section 5](#); [Annex 2 to the AEO Guidelines point 4](#))*

**Note:**

This section concerns the security & safety criterion for AEO. It should **only** be completed if you are applying for an AEOS authorisation. The self-assessment for this requirement shall comprise all the premises which are relevant to the customs related activities of the applicant.



You should demonstrate a high-level of awareness on security and safety measures, internally and in your business activities with clients, suppliers and external service providers, considering your role in the international supply chain.

You should not confuse this with health & safety requirements (please see AEO Guidelines).

Normally any procedures referred to in this Section are expected to be of a sufficient standard and detail to (a) clearly identify both the responsible person and their deputy(ies) and (b) to enable the deputy(ies) to act in the way designated by the responsible person.

All procedures should be documented and made available for customs authorities during the audit of the AEO criteria and will always be checked on site.

The documents you are required to produce, particularly at 6.1.2(a) & (b), should reflect:

- your role in the international supply chain
- the nature & size of your business; and
- the risks and threats to your business.

### **Subsection 6.1 – General information on safety and security**

**6.1.1.** According to Article 28 (1) (h) UCC IA, a contact person competent for safety and security related questions has to be appointed. In this context safety and security only refers to that of the AEO criterion. It is to be noted that it is not related to the “safety at work” as this is out of the scope of the safety and security criterion.

#### **6.1.2 (a)**

Customs authorities expect a documented risk and threat assessment to have been carried out by either you or a security company, in case you use one. Failure to produce this assessment at their visit may result in an automatic recommendation that the application be rejected. The risk and threat assessment shall cover all the premises which are relevant to your customs related activities. The purpose of the assessment is to identify the risks and threats which might occur in that part of the international supply chain in which you operate, and to look into the measures in place to minimise the risks and threats. It should cover all the risks related to the security of your role in the international supply chain and should include, for example:

- physical threats to premises and goods

- fiscal threats
- contractual arrangements for business partners in your supply chain.

Such an assessment should address the following:

- the goods in which you deal/trade
- specific management of air cargo/air mail if concerned (access, handling, storage, etc.)
- premises and buildings, for storage, manufacture etc.
- staff including recruitment, use of temporary staff, sub-contract labour
- transport of goods, loading and unloading
- computer system, accounting records and documents
- recently reported security incidents in any of the areas above.

You should also provide evidence of how often the document is reviewed and updated and procedures should include how to report incidents and the frequency of future reviews. Customs shall also seek evidence of how and when your procedures are communicated to both staff and visitors.

#### **6.1.2 (b)**

Failure to produce either a security plan or a risk and threat assessment at the visit of the customs authority may result in premature termination of the visit or rejection of the application.

A review programme should be in place for the security plan which should include records of amendments which are signed and dated by the responsible person.

#### **6.1.3**

You should include a description of at least the top five perceived risks you have identified. The customs authorities would expect you to have assessed and included these risks within your risk and threat assessment, covering their likelihood, the consequences and any countermeasures. Examples of these could be:

- smuggling illicit goods
- contamination of products
- tampering with goods for export
- unauthorised access etc.

#### **6.1.4**

Describe briefly the process for setting up security measures, implementing, monitoring and reviewing them. You will need to identify the responsible person and his tasks. There should be one person at the appropriate level within the organisation with overall responsibility for all security measures and with the necessary authority to implement appropriate security measures when required. If not, indicate the various departments involved and the overall coordination and management.

If external security services are used, the responsible person should manage the contract and ensure a proper service level agreement is in place that meets the AEO requirements as demonstrated by the questions in this Section.

The responsible person should be able to explain and have adequate procedures in place for drafting, reviewing and updating all security measures. This person would normally be responsible for preparing the documents required at question 6.1.2 (a) & (b).

The customs authorities would expect the procedures to be sufficient to enable any person deputising for the responsible person both to accept responsibility and undertake the task required.

#### **6.1.5**

Although in many cases security measures are likely to be site specific, the governance procedures for setting-up, implementing, monitoring and reviewing the measures may be harmonised across all locations. Where measures are not harmonised this may increase the number of site visits carried out by the customs authorities.

#### **6.1.6 (a) & (b)**

You should have documented procedures in place to enable and encourage staff and if possible also visitors to report any security incidents, for example, unauthorised access, theft, use of unchecked personnel. This should include how this is to be done, to whom and where they are located. Your procedures should also detail how such incidents should be investigated, reported upon and by whom.

If you have answered “No”, please indicate how you intend to address this and indicate the time scale.

A “Yes” answer should be accompanied by your explanation as to how safety instructions are communicated to staff and should include details as to how you ensure your staff has seen them. You should also explain how security instructions are brought to the attention of your visitors.

See also question 6.3.2.

References to “Security” instructions should not be confused with any instructions required for health & safety reasons and made clear to visitors and staff.

#### **6.1.7 (a) & (b)**

This question relates to international supply chain security and not health & safety incidents.

For example:

- losses in warehouse
- broken seals
- damaged anti-tampering devices

If there have been any incidents the customs authorities will expect your security and safety procedures to have been reviewed and amended to take on board any remedial action. Evidence will also be required of how these changes were subsequently communicated to your staff and visitors.

If following any review of your security & safety procedures any amendments are made, these should be recorded as a revision with a record of the date and the part(s) revised.

#### **6.1.8 (a), (b) & (c)**

You should ensure you hold the original documentation, including the assessment report, if it is available, as this may be requested by customs authorities during the on-site visit. The relevant certification will be taken into account by the customs authorities when they prepare and conduct the audit.

For example:

- Regulated Agent (certificate and assessment report)
- Known Consignor (certificate and assessment report)
- TAPA (certificate and assessment report)
- ISO (certificate and quality manual)
- ISPS

#### **6.1.9**

Your answer should include for example details as to any hazardous chemicals, high value goods, or excise goods and explain whether these are on a regular or irregular basis.

For example:

- special packaging
- specific storage requirements

See also 6.5.1 (logistic processes).

#### **6.1.10 (a) & (b)**

Your answer should include the name and address of the company(ies) and indicate how many years it (they) has (have) been employed by you as your security company and whether they provide any other services for you.

If the company has made a threat assessment, your reply should also confirm that any risks identified have been incorporated into your risk and threat assessment covered by question 6.1.2 (a).

The documents should show the date(s) when the assessment was conducted and implementation of any recommendations made. The document should be made available during the visit.

#### **6.1.11**

Your reply should give an indication of the different customers/insurance company requirements and the goods affected by any special requirements e.g. particular packaging or storage requirements.

If you have a wide range of products and requirements it will be sufficient to summarise them. They will be examined in more detail during the visit.

### **Subsection 6.2 – Building Security**

In order to comply with the criterion mentioned in Article 28 (1) a UCC IA, you should ensure that buildings used in connection with the operations relating to the AEOS authorisation provide protection against unlawful intrusion and are constructed of materials which resist unlawful entry.

#### **6.2.1 (a) (b) & (c)**

This also applies where you have visible external boundaries to your premises, for example, fences and gates. The customs authorities would expect all external and internal windows, gates and fences to be secured with e.g. locking devices, alternative access monitoring or control measures such as internal/external anti burglar alarm systems or CCTV (Closed Circuit TV systems).

For questions (a) to (c) - details as to how compliance with these procedures are checked, the frequency of checks to buildings and any fences, the security incidents are reported and dealt with should be contained within the document required in answers 6.1.2.(a) or (b). Provide reference here to the appropriate paragraph, section or page (revision/date) of that document.

#### **6.2.2 (a) & (b)**

You should list all access points, preferably with reference to the site plan; include any fire escapes showing access stairways; distinguish between those accesses designed for cargo (un)loading those for utilities, counters for public access, drivers' rest areas; state where any security guard offices/guardhouse is located.

Your description of how these are observed should include, where appropriate, the type of CCTV (e.g. static camera or pan tilt and zoom), how they are controlled and whether the image is used proactively or reactively.

In addition to external access controls you should also describe internal access controls, including, where appropriate, internal access within shared premises.

Confirm whether the premises operate 24/7 (e.g. shift working) or normal office hours.

### **6.2.3**

If appropriate also include details of any back-up generators or devices in place to ensure constant lighting to cover when local power supply is interrupted and how this is maintained.

### **6.2.4**

How keys are identified and what are the procedures in place to prevent misuse and deal with any loss.

Procedures should exist for only authorised personnel to have access to keys to locked buildings, sites, rooms, secure areas, filing cabinets, safe, vehicles and machinery. Your procedures should also include:

- the specially appointed place where the keys are kept
- the person responsible for controlling the security of the keys
- the recording of when the keys are taken, by whom, why and their return
- dealing with losses, failures to return keys.

0

Provide details of any lock-up procedures and, if appropriate, who are the master key holders responsible for closing down the premises at night and re-opening on the next working day.

Provide details of other “key” devices as “radio keys” (used for example to remotely operate a car park barrier) in use and to whom they have been issued.

### **6.2.5 (a), (b), (c) & (d)**

Your procedures should include:

- how you control/record visitors with private vehicles attending your premises
- how you control staff vehicles at your premises
- specially designated car park areas for visitors and staff which are not close to secure areas, for example, loading bays to avoid the possibility of theft, obstruction or interference
- checks that parking requirements are being adhered to.

- (a) Explain whether visitors' cars are segregated from staff cars. You should include details of any other vehicles which have temporary access to the site(s) for example taxis or a staff bus.
- (b) You should ensure that there are procedures in place to ensure the authorisation is regularly reviewed and updated to take into account changes of staff cars. Provide details if staff are issued with a parking permit and the mechanism for entering / exiting the car park, for example a card swipe barrier.
- (c) Describe any process or procedure employed for vehicle checking, for example if barriers are manned during peak hours to control tail-gating and ensure proper control of all vehicles.
- (d) Describe any written regulations covering car parking and how these are communicated to the staff. Confirm whether such regulations have been included in the security assessment.

### **Subsection 6.3 – Access to premises**

To avoid tampering with goods the applicant shall according to Article 28 (1) (b) UCC IA have appropriate measures in place to prevent unauthorised access to offices, shipping areas, loading docks, cargo areas and other relevant places.

#### **6.3.1 (a) & (b)**

You should briefly describe the process making it clear, where necessary, if any site specific processes are involved. For a multi-site application it may be helpful to describe or provide an image of a general view of the sites. Your procedures should document who has access to which areas, buildings, and rooms and how this is controlled, for example, by keypads or swipe cards. Access restrictions should take into account the risk and threat assessment at 6.1.2a.

Your systems should be capable of identifying attempts at unauthorised access and to monitor these.

Describe the system used to identify staff and distinguish from visitors, e.g. identity cards.

#### **6.3.2 (a) & (b)**

Your reply should confirm the details by reference to the risk and threat assessment described in 6.1.2 (a) & (b). You should include details of any cooperation with other security organisations/ law enforcement agencies who share knowledge of such matters.

Please also refer to your reply given at 6.1.6 and the explanatory notes contained there.

#### **6.3.3**

A site plan should be made available for the customs authorities. Whilst a plan is not mandatory, any illustration will assist them in preparation for the audit and may reduce the time required during the on site(s) visit.

The plan could be or include a satellite/internet image of the site if available.

Any image or plan presented should contain the date when produced and be otherwise uniquely identifiable to form an audit trail for the AEO application.

#### **6.3.4**

You should pay particular attention to any companies on your site who are merely tenants rather than involved in making supplies to or for you. Tenants may pose special security issues and any arrangements covering for example their segregated entry and occupancy within your area should be briefly described.

Please also refer to 6.12.

### **Subsection 6.4 - Cargo Units**

In order to comply with the criterion mentioned in Article 28 (1) (c) UCC IA, measures for the handling of goods which include protection against the unauthorised introduction or exchange, the mishandling of goods and against tampering with cargo units have to be taken.

Cargo units include containers, tankers, vans, lorries, vehicles, pipelines and so on in which your goods are transported. Procedures should be in place to examine the integrity of the cargo unit before loading. Details of the owners/suppliers of the cargo units must be made available during the visit.

#### **6.4.1**

The integrity of cargo units should be ensured, for example, by placing them under permanent monitoring or keeping them in a safe, locked area or by inspection prior to use. Only properly identified and authorised persons should have access to the cargo units. Your procedures should include:

- how access to the area where the cargo units are held is controlled (e.g. staff, external truck drivers, etc.)
- that only authorised persons have access
- how monitoring of the units is maintained at all times, for example, nominated responsible staff and deputies.

#### **6.4.2**

Your procedures should include:



- who is the responsible person to whom incidents are reported
- how incidents are reported and recorded
- what action should be taken, including reporting to law enforcement/senior management
- review and amending of existing procedures
- notification of any changes to staff.

Customs authorities would expect to see evidence of these checks during the visit.

#### **6.4.3 (a) & (b)**

Describe the type of seals used and any standards satisfied by the particular seals used. Provide the name of the manufacturer, the procedure for issuing seals and for recording their issue, usage and removal.

Document the procedures for dealing with broken and tampered seals.

#### **6.4.4**

Depending on the cargo unit used, a seven-point inspection process should be carried out (to include the tractor unit as well):

- front wall
- left side
- right side
- floor
- ceiling/roof
- inside/outside doors
- outside/undercarriage.

#### **6.4.5 (a) – (d)**

Maintenance should be done routinely not just in cases of damage or incidents. If the maintenance is done externally or outside the supervision of your staff, the cargo unit's integrity should be inspected when returning to your premises. Your procedures should include:

- the requirements for your staff to check the integrity of the units on their return
- what checks are to be performed, when and by whom
- how your procedures are communicated to staff
- management checks and their frequency to ensure units are re-examined.

Explain whether you routinely check all cargo units both before accepting any incoming load and before loading goods for despatch and whether you have inserted procedures within the documents referred to in 6.1.2 (a) and (b).

## **Subsection 6.5 – Logistical Process**

### **6.5.1 (a) - (d)**

This covers the movement of your imported and/or exported goods between your premises and the frontier, across the EU and within different sets of premises.

You should list all modes of transport used starting or ending within your premises and entering the international supply chain. Indicate the mode of transport used.

If you use external service providers, please also refer to 6.12 (External services).

## **Subsection 6.6 – Incoming goods**

In order to comply with the criterion mentioned in Article 28 (1) (b) UCC IA appropriate access control measures should be put in place to prevent unauthorised access to shipping areas, loading docks and cargo areas.

### **6.6.1 (a) & (b)**

These procedures should start from the point of placing an order through to delivery for the international supply chain.

Documented procedures should show the flow of goods and related documents and include other parties involved such as suppliers, packers, hauliers etc.

### **6.6.2**

When there are existing arrangements on security measures with domestic and/or EU and non-EU suppliers, staff should be made aware of these arrangements and procedures established to verify the commitment to them. You should describe the process whereby employees are informed about security, the frequency of any retraining and consider the evidence required to demonstrate this to the visiting officer and for any AEO review.

Your procedures should also include:

- appointing staff responsible for receiving the driver and the goods at arrival
- maintaining a schedule of expected arrivals
- dealing with unexpected arrivals

- recording the transport documents and customs papers accompanying the goods
- comparing the goods with the accompanying transport documents and customs papers
- checking the integrity of any seals
- recording the completion and results of any checks
- informing customs authorities as required on arrival of the goods to enable them to perform the necessary controls
- weighing/counting and tallying the goods against the picking list/purchase order
- testing quality
- the goods are adequately marked before going into stock to enable identification
- identification and reporting of discrepancies or quality control failures
- informing the purchase department and the administration of the receipt of goods.

For example, this may depend on if you are dealing in high value/risk goods. Arrangements may be that the goods:

- must arrive in the same condition they left the supplier
- be sealed at all times
- have not breached any security or safety requirements.

Your procedures should include:

- communicating such arrangements to staff responsible for receiving incoming goods so that they are aware of what to do in particular if an irregularity is discovered
- reviewing and updating these procedures on a regular basis
- management/supervisory checks to ensure staff are following these requirements.

#### **6.6.3 (a) and (b)**

On arrival of the sealed cargo unit measures should be in place to ensure correct treatment of the seal. These could include a visual inspection to ensure a) that the seal is actually intact and b) there is no evidence of tampering. Once satisfied from a visual inspection the authorised person could then proceed to physically test the seal by suitable pressure applied to ensure it is still intact.

#### **6.6.3 (c)**

In case your company is dealing with specific types of goods requiring specific security measures (e.g. air cargo/air mail) your procedures should include how you apply them/check their application. For example, in case you are regulated agent whether and how you check the haulier declaration and the identity of the haulier for the transportation of secure air cargo/air mail from a known consignor.

### **6.6.5**

Depending on the nature of the goods in which you deal counting, weighing or quantification may not be appropriate. An alternative method for accounting for incoming goods should be described and how compliance is evidenced.

### **6.6.6**

Your procedures should include:

- how and on the basis of which documents, when and by whom are the goods received entered in the stock records
- checking the goods against loading lists and purchase orders
- recording the goods in the stock record, as soon as possible after their arrival.

### **6.6.7 (a) & (b)**

There should be a segregation of duties between the ordering of the goods (purchase), receipt (warehouse), the entering of the goods in the system (administration) and the payment of the invoice. This will depend upon the size and complexity of the business.

## **Subsection 6.7 – Storage of goods**

**This sub-section only covers the storage of goods that are part of an international supply chain.**

### **6.7.1 - 6.7.5**

Your procedures should include:

- a designated area for storage of the goods which is both safe and secure and clearly known to controlling staff
- storage area only accessible to authorised staff
- regular stock takes
- controlling incoming goods, transfers to other premises, permanent and temporary removals
- action to be taken if irregularities, discrepancies, losses or theft are identified
- handling and processing of goods and their return to stock
- separation of different types of goods, where appropriate, for example, Union, non-Union, high value, hazardous, air cargo/air mail
- maintaining and updating stock records promptly including the location of the goods

- addressing all aspects of physical security of the storage facility.

Standards of security will depend on the type of goods, size and complexity of the business which could range from a single room in a block of offices to a large multi-sited business operating in several MS.

#### **6.7.6**

In case of subcontracting, please indicate the company(ies) in charge of the storage.

### **Subsection 6.8 – Production of goods**

**This sub-section only covers the production of goods that form part of an international supply chain.**

Only complete questions 6.8.1 – 6.8.4 if it is appropriate to your business. Production in this context can include a range of activities such as manufacturing from raw materials through to assembly from bought in parts.

#### **6.8.1 (a) & (b)**

Include within your description whether staff working within the production area are permanent employees of the business or temporary staff. Describe the location of the production within your premises and if possible, indicate its location on a copy of the site plan. Please also refer to notes 6.2.3.

#### **6.8.2**

Support your answer by reference as appropriate to the risk and threat assessment described at question 6.1.2 (a) & (b). Any compliance checking should be supported by suitable evidence which is signed and dated.

#### **6.8.3**

Include any reference to technological aids to packing integrity (e.g. weight checked or CCTV surveillance etc). Also describe any securing process both of the individual packages and how the packages are consolidated, for example palletized. Provide details as to the point at which the consignee (address/country) is known and how this knowledge is controlled.

#### **6.8.4**

Your description should include reference to any contractual and or service level agreements with the third party. The customs authorities will wish to see these.

This also includes where packages may be consolidated.

## **Subsection 6.9 – Loading of goods**

### **6.9.1 (a) & (b) and 6.9.2 (a), (b) & (c)**

Personnel should be assigned to supervise the loading of goods to prevent goods being loaded unsupervised or left behind. Your procedures should include:

- appointing staff responsible for receiving the driver and the loading of the goods
- assigned staff are present at all times
- procedure if assigned staff not available, for example, appointment of deputies
- loading only taking place in the presence of authorised staff
- weighing, counting, tallying and marking of goods
- dealing with discrepancies/irregularities
- the application of seals and recording on documents/records, ensuring that seals have been used for appropriate goods, meet laid down standards and applied in accordance with legal requirements
- recording the transport and customs documents accompanying the goods in your records
- comparing the goods with the accompanying transport and customs documents
- recording the completion and results of the checks
- informing customs authorities as required on departure of the goods to enable them to perform the necessary controls
- informing the selling department/administration on the departure of goods
- how (on the basis of which documents), when and by whom are the goods loaded recorded in the stock records
- checking the goods against loading lists and selling orders
- recording the goods out of the stock, as soon as possible after departure of the goods
- acknowledging receipt of the goods and any irregularities by your customers
- proof of export where appropriate.

### **6.9.3**

This will only apply if your customers have agreed specific requirements with you, for example, all goods must be sealed, packed and labelled in a certain way for X-ray requirements. If so, staff should be made aware of these arrangements and your procedures should include management/supervisory checks to ensure staff are following these requirements. These procedures should be reviewed and updated on a regular basis.

See also 6.1.11 answer.

### **6.9.7**

Evidence to support this section should be referenced to the appropriate area in the risk and threat assessment described under question 6.1.2. (a) & (b).

Irregularities may include customer returns, unauthorised drivers, broken anti-tampering devices, etc.

### **Subsection 6.10 – Security requirements for business partners**

**In order to comply with the criterion mentioned in Article 28 (1) (d) UCC IA, you should have taken measures allowing to clearly identify your business partners and to ensure, through implementation of appropriate contractual arrangements or other appropriate measures in accordance with your business model, that those business partners ensure the security of their part of the international supply chain.**

Business Partners can be suppliers (of goods or services) or customers.

#### **6.10.1**

Your answer would be expected to be supported by documentary evidence. Customs authorities would expect to see whatever documentary evidence you have in support of the reply provided. Such documents would include your record of checks applied. These should be made available for inspection during the visit.

#### **6.10.2 (a) & (b)**

You are primarily responsible for your part of the international supply chain, for the goods which are under your control and for the facilities you operate. Nevertheless, the security of the international supply chain depends also on the security of your business partners and you shall make any possible effort to ensure that your business partners comply with the security AEO requirements.

Requirements for your suppliers could include for example that all goods must be marked, sealed, packed, labelled in a certain way, subject to X-ray checks etc. and that they keep to any laid down international standards.

Where such requirements exist, your procedures should include:

- where possible, regular visits to the supplier's business premises to verify requirements are being adhered to
- communicating these arrangements to your staff to check compliance on arrival of the goods
- arrangements for staff to report irregularities/incidents
- management/supervisory checks to ensure staff are following these requirements
- remedial action taken as a result of any identified breaches of these arrangements
- review and update of procedures on a regular basis.

Customs authorities would expect to see whatever documentary evidence you have in support of the reply provided. Such documents would include your record of checks applied. These should be made available for inspection during the visit.

### **6.10.3**

Your answer would be expected to be supported by documentary evidence. Customs authorities would expect to see whatever documentary evidence you have in support of the reply provided. Such documents would include your record of checks applied. These should be made available for inspection during the visit.

Customs authorities would expect that any such breaches would be reflected in the documents identified at 6.1.2 (a) & (b) together with a suitable revision and additional countermeasure(s).

## **Subsection 6.11 – Personnel security**

In order to comply with the criterion mentioned in Article 28 (1) (e) and (g) UCC IA you should:

- a) have conducted, in so far as national law permits, security screening on prospective employees working in security sensitive positions and carry out background checks of current employees in such positions periodically and where warranted by circumstances;
- b) ensure that your staff having responsibilities relevant for security issues regularly participate in programmes to raise their awareness of those security issues.

### **6.11.1 (a), (b) & (c)**

Your employment policy should reflect your security requirements based on your risk assessment. Your procedures should include:

- performing background checks on your new and existing employees who will be working in or moving to security sensitive positions
- seeking and taking up references on recruitment
- identifying critical security posts and carrying out necessary checks to include both spent and unspent convictions



- requirement by staff to notify their manager of police cautions/bail, pending court proceedings, convictions
- removal of computer access, return of security pass when staff leave or are dismissed
- disclosure by staff of any other employment.

Any compliance checking should be properly evidenced by initial and date on a suitable record of checks applied.

#### **6.11.2 (a) & (b)**

Procedures should be in place within the documents referred to in 6.1.2. (a) & (b). These should cover how prospective new employees are checked before offering employment; the process of induction and training which should include the company's security instructions. All new staff should sign to indicate their understanding of the issues. Procedures should also cover what measures are taken in case existing employees are transferred to security sensitive areas.

#### **6.11.3 (a), (b), (c) & (d)**

All staff should receive appropriate training with regard to security and safety requirements, such as security protocols, detection of intrusion/tampering and reporting of incidents and the risks associated to the international supply chains. A unit or a group of persons (internal or external) should be responsible for providing training to the staff. Training should be updated if there are changes and a record made of all training activity should be maintained.

For any external supplier a suitable Service Level Agreement should be obtained. Please also refer to 6.12.1.

#### **6.11.4 (a) & (b)**

The company should have security requirements in place regarding the use of temporary personnel. Your procedures should include:

- contracts with employment agencies detailing levels of security checks to be performed on staff prior to and after appointment
- use of only known agencies who meet requirements
- similar security standards for both temporary and permanent staff (see note 6.11.1).

You must make available all such contracts during the visit.

Customs authorities would expect all temporary staff to have been checked to the same standard as permanent staff. As it is common for such staff to be procured by an external temporary staff agency, such agencies should be subject to service level agreements (see also 6.12) and procedures should exist to ensure standards provided for in these agreements are maintained by the company and evidenced within your records.

### **Subsection 6.12 – External services**

Article 28 (1) (f) UCC IA requires you to have appropriate security procedures in place for any external service providers contracted. Such service providers could include areas as transportation, security guards, cleaning and maintenance. the external contractors.

**6.12.1 (a), (b) and (c)**

For questions (a) to (b) - you should have ready for the visit of the customs authorities all contracts and service level agreements covering identity checks on employees and other matters with all such external services. Please provide a list of all companies and indicate the services they provide during the visit.

For question (c) - describe how you monitor the contract, handle any irregularities and review the procedures. Support your answer by reference, as appropriate, to the risk and threat assessment described under question 6.1.2 (a) & (b). Any compliance checks should be supported by suitable evidence which is signed and dated.

**Annex 1**

**Consent to disclose the AEO details on the TAXUD website**

I hereby give my consent to the publication of the information in the AEO authorisation in the list of authorised economic operators.

Signature.....  
Capacity of Signatory.....  
(The completed questionnaire should be signed by a Director/Managing Partner/Sole Proprietor as appropriate but for this case it is recommended that consent is given by an authorised signatory)  
Date:.....

**Consent to the exchange of the information in the AEO authorisation in order to ensure the implementation of international agreements with third countries on mutual recognition of the status of authorised economic operators and measures related to security**

I hereby give my consent to the exchange of the information in the AEO authorisation in order to ensure the implementation of international agreements with third countries on mutual recognition of the status of authorised economic operators and measures related to security:

Signature.....  
Capacity of Signatory.....  
(The completed questionnaire should be signed by a Director/Managing Partner/Sole Proprietor as appropriate but for this case it is recommended that consent is given by an authorised signatory)  
Date:.....

If you have provided your consent for mutual recognition please also provide the following information:

Transliterated name:.....  
Transliterated street and number:.....  
Transliterated postal code and city:.....

Only Latin characters should be used as codified in <http://www.unicode.org/charts/PDF/U0000.pdf>

**Annex 2**

**Table of criteria that apply to different actors in the international supply chain**

		<b>Manufacturer</b>	<b>Exporte r</b>	<b>Freight Forwarder</b>	<b>Warehous e keeper</b>	<b>Custom s broker</b>	<b>Carrier</b>	<b>Importer</b>
<b>0</b>	<b>General Information</b>							
0.1.	Guidelines for Authorised Economic Operators	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
0.2.	Inclusion of company's departments	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
<b>1</b>	<b>Company information</b>							
1.1.	General Company information (1.1.1. to 1.1.11. only to be filled in, if not already answered in the obligatory information in the AEO application)	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
1.1.1.	Name, address, date of establishment and legal form of the organisation of the applying company	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
1.1.2.	Full details of main shareholders, board members and/or managers	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
1.1.3.	Name of the person in charge of the applicant's customs matters	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

1.1.4.	Commercial activity and position in the international supply chain	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.1.5.	Specification of locations	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.1.6.	Associated businesses	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.1.7.	Description of the company's internal organisational structure and the tasks/responsibilities of each department	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.1.8.	Names of senior management	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.1.9.	Number of employees	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.1.10a	Consent publication on TAXUD websited	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.1.10b	Consent Mutual recognition	<b>AEOC</b>	<b>AEOC</b>	<b>AEOC</b>	<b>AEOC</b>	<b>AEOC</b>	<b>AEOC</b>	<b>AEOC</b>
		<b>Manufacturer</b>	<b>Exporte r</b>	<b>Freight Forwarder</b>	<b>Warehous e keeper</b>	<b>Custom s broker</b>	<b>Carrier</b>	<b>Importer</b>
1.2.	Volume of business							
1.2.1.	Annual turnover figure - profit or loss	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.2.2.	Storage facility	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.2.3.	Number and value of the customs declarations	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.2.4.	Amount of duty	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
1.2.5.	Foreseen structural changes in your company	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC

**Annex 1b**  
**to TAXUD/B2/047/2011- REV6**

1.3.	Statistics on customs matters							
1.3.1.	Representation in customs matters		AEOC / AEOs			AEOC / AEOs		AEOC / AEOs
1.3.2.	Tariff classification of goods	AEOC / AEOs*	AEOC / AEOs			AEOC / AEOs		AEOC / AEOs
1.3.3.	Establishment of customs value	AEOC / AEOs*	AEOC / AEOs*			AEOC / AEOs		AEOC / AEOs
1.3.4.	Origin of goods	AEOC / AEOs*	AEOC / AEOs			AEOC / AEOs		AEOC / AEOs
1.3.5.	Anti-dumping duties or countervailing duties	AEOC / AEOs*				AEOC / AEOs		AEOC / AEOs
<b>2</b>	<b>Compliance record</b>							
2.1.	Detected breaches of customs and taxation rules	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
2.2.	Applications for other customs authorisations and certifications	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
<b>3</b>	<b>The applicant's accounting and logistical system</b>							
3.1.	Audit trail							
3.1.1.	Essential features of audit trail	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.2.	Accounting and logistical systems							

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

3.2.1.	IT-equipment	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
3.2.2.	Differentiation between Union-/non-Union goods	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
3.2.3.	Location of computer activities	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
		<b>Manufacturer</b>	<b>Exporte r</b>	<b>Freight Forwarder</b>	<b>Warehous e keeper</b>	<b>Custom s broker</b>	<b>Carrier</b>	<b>Importer</b>
3.3.	Internal control system							
3.3.1.	Internal control procedures	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
3.3.2.	Audit of internal control procedures	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
3.3.3.	Checking of computer files	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
3.4.	Flow of goods							
3.4.1.	Registration process	AEOC / AEOC	AEOC / AEOC		AEOC / AEOC			AEOC / AEOC
3.4.2.	Checking stock levels	AEOC / AEOC	AEOC / AEOC		AEOC / AEOC			AEOC / AEOC
3.5.	Customs routines							
3.5.1.	Verification of customs declarations	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC	AEOC / AEOC*
3.5.2.	Notification of irregularities	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
3.5.3.	Economic trade licences	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC*	AEOC / AEOC	AEOC / AEOC*
3.5.4.	Goods subject to import and export licenses connected to prohibitions and restrictions	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

3.5.5	Goods falling under the Dual Use Regulation	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.6.	Procedures for back-up, recovery and fall back and archiving							
3.6.1.	Back-up and archiving of data	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.6.2.	Duration of archiving	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.6.3.	Contingency plan	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.7.	Protection of computer systems							
3.7.1.	Protection from unauthorised intrusion	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.7.2.	Administration of access rights	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.7.3.	Main server	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.8.	Documentation security							
3.8.1.	Protection of documents from unauthorised access	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.8.2.	Cases of unauthorised access	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs
3.8.3.	Access for different categories of employees	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs	AEOC / AEOs



**Annex 1b  
to TAXUD/B2/047/2011- REV6**

3.8.4.	Security & safety requirements for third parties	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
		<b>Manufacturer</b>	<b>Exporter</b>	<b>Freight Forwarder</b>	<b>Warehouse keeper</b>	<b>Customs broker</b>	<b>Carrier</b>	<b>Importer</b>
<b>4</b>	<b>Financial solvency</b>							
4.1.	Insolvency proceedings	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
4.2.	Financial standing	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
4.3.	Newly established business	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
4.4.	Financial solvency in the foreseeable future	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC	AEOC / AEOC
<b>5</b>	<b>Practical standards of competence or professional qualifications</b>							
5.1.	Practical standards of competence							
5.1.1.	Practical experience of a minimum of three years in customs matters	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
5.1.2.	Quality standard concerning customs matters adopted by a European Standardisation body	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
5.2.	Professional qualifications							

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

5.2.1.	Successfully completed training covering customs legislation consistent with and relevant to the extent of your involvement in customs related activities	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
<b>6</b>	<b>Safety and security requirements</b>							
6.1.	<b>General information on safety and security</b>							
6.1.1	Person competent for safety and security related questions	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.2.	Risk and threat assessment	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.3.	Security risks	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.4.	Implementation of security measures	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.5.	Harmonisation of security measures	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.6.	Security instructions	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.7.	Security incidents	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.8.	Certification for security purposes by another public agency or authority	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.9.	Particular security and safety requirements for the goods	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.10.	Threat assessment by third parties	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC
6.1.11	Safety and security requirements imposed by third parties	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC	AEOC

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

6.2.	Building security							
6.2.1.	Safety of external boundaries of your company's premises	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.2.2.	Access possibilities	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.2.3.	Illumination	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.2.4.	Access to keys	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.2.5.	Parking of private vehicles	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.3.	Access to premises							
6.3.1.	Access controls	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.3.2.	Procedures in case of unauthorised intrusion	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.3.3.	Site plans of locations	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.3.4.	Companies located at the premises	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
		<b>Manufacturer</b>	<b>Exporte r</b>	<b>Freight Forwarder</b>	<b>Warehous e keeper</b>	<b>Custom s broker</b>	<b>Carrier</b>	<b>Importer</b>
6.4.	Cargo units (as containers, swap bodies, transport boxes)							
6.4.1.	Rules for access to cargo units	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.4.2.	Measures to ensure the integrity of cargo units	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

6.4.3.	Use of seals	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.4.4.	Measures used for checking cargo units	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.4.5.	Owner/operator and maintenance of cargo units	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.5.	Logistical processes							
6.5.1.	Means of transport	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.6.	Incoming goods							
6.6.1.	Procedure for checking of incoming goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.6.2.	Security arrangements with suppliers	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.6.3.	Checks on the integrity of the seals	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.6.4.	Uniform marking of goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.6.5.	Weighing and counting of goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.6.6.	Procedure for the receipt of goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.6.7.	Internal control procedures	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.7.	Storage of goods							
6.7.1.	Areas for the storage of goods	AEOS	AEOS	AEOS*	AEOS	AEOS	AEOS	AEOS*
6.7.2.	Allocation of a storage position	AEOS	AEOS	AEOS*	AEOS	AEOS	AEOS	AEOS*
6.7.3.	Internal control	AEOS	AEOS	AEOS*	AEOS	AEOS	AEOS	AEOS*

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

	procedures							
6.7.4.	Separate storage of different kinds of goods	AEOS	AEOS	AEOS*	AEOS	AEOS	AEOS	AEOS*
6.7.5.	Protection against unauthorised access	AEOS	AEOS	AEOS*	AEOS	AEOS	AEOS	AEOS*
6.7.6.	Control measures in case of outsourced storage	AEOS	AEOS	AEOS*	AEOS	AEOS	AEOS	AEOS*
6.8.	Production of goods							
6.8.1.	Designation of production areas	AEOS						
6.8.2.	Security measures for access to the production zone	AEOS						
6.8.3.	Packing of products	AEOS	AEOS*					
6.8.4.	Packing by third parties	AEOS	AEOS*					
		<b>Manufacturer</b>	<b>Exporte r</b>	<b>Freight Forwarder</b>	<b>Warehous e keeper</b>	<b>Custom s broker</b>	<b>Carrier</b>	<b>Importer</b>
6.9.	Loading of goods							
6.9.1.	Management of loading	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	
6.9.2.	Sealing of outgoing goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	
6.9.3.	Customers' security requirements	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.9.4.	Supervision of loading of goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.9.5.	Weighing and counting of goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.9.6.	Procedure for the loading of goods	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.9.7.	Control measures	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS

**Annex 1b  
to TAXUD/B2/047/2011- REV6**

6.10.	Security requirements for business partners							
6.10.1.	Verification of business partners	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.10.2.	Security and safety requirements for business partners	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.10.3.	Breaches of security agreements	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.11.	Personnel security							
6.11.1	Security and safety requirements in the employment policy	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.11.2	Security checks on employees	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.11.3	Security and safety training	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.11.4	Security requirements in case of temporary employees	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS
6.12.	External Services							
6.12.1	Use of external services	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS	AEOS

\* Where appropriate

## Threats, Risks and Possible solutions

This document provides a list of the most significant risks related to the AEO authorisation and monitoring process, and at the same time, it provides a list of possible solutions on how to keep these risks under control. Possible solutions proposed for one indicator can be applicable to more than one risk area identified. The suggested list is neither exhaustive nor definitive and possible solutions will in practice vary from case to case. They will be influenced by and have to be proportional to the size of the operator, type of goods, type of automated systems and level of modernization of the operator.

The self-assessment questionnaire is completed by the economic operators at the very beginning of the application process and aims to give a state of play of their business and procedures and their relevance for the AEO authorisation. The ‘Threats, risks and possible solution’ document is addressed both to customs authorities and economic operators to facilitate the audit and examination to ensure compliance with AEO criteria by matching the information provided in the [SAQ](#) and the risk areas identified and possible solutions to cover them.

### 1. Compliance record ([Section 2 from the SAQ](#))

Criterion: An appropriate record of compliance with customs requirements (Articles 39 (a) UCC and 24 UCC IA)

Indicator	Risk description	Possible solutions	References
Compliance with customs requirements	Non-compliant behaviour with regard to: - fulfilment of customs declarations including incorrect classification, valuation, origin, - use of customs procedures - taxation rules, - application of measures related to prohibitions and restrictions, commercial policy, - introduction of goods to the customs territory of the	active compliance policy by the operator in the sense that the operator has its internal rules for compliance in place and implemented; written operating instructions are preferred as regards responsibilities for carrying out checks on accuracy, completeness and timelines of transactions and disclose irregularities/errors, including suspicion of criminal activity to customs authorities; procedures to investigate and report errors found and to review and improve processes; the competent/responsible person within the business should be clearly identified and arrangements for cases of holidays or other types of absences should be installed;	<a href="#">SAQ - 2.1</a>

<p>Community etc. Non-compliant behaviour in the past increases the chance that future rules and regulations will be ignored/violated. Insufficient awareness of breaches against customs requirements.</p>	<p>implementation of internal compliance measures; use of audit resources to test/assure procedures are correctly applied; internal instructions and training programmes to ensure staff are aware of customs requirements.</p>	
---	---	--

2. The applicants accounting and logistical system ([Section 3 from SAQ](#))

Criterion: A satisfactory system of managing commercial and where appropriate, transport records, which allow appropriate customs controls (Articles 39 (b)UCC and 25 UCC IA)

2.1. Accounting system ([Subsection 3.2 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Computerised environment	<p>The risk that an accounting system is inconsistent with the generally accepted accounting principles applied in the Member State. Incorrect and/or incomplete recording of transactions in the accounting system. Lack of reconciliation between stock and accounting records. Lack of segregation of duties between functions.</p>	<p>segregation of duties between functions should be examined in close correlation with the size of the applicant. For example, a micro-enterprise which is performing road transport business with a 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); implement a warning system which identify suspicious transactions;  develop interface between customs clearance and accounting software to avoid typing errors;</p>	<p><a href="#">SAQ - 3.2</a> ISO 9001:2015, section 6</p>
Integrated accounting system	<p>Lack of physical or electronic access to customs and, where appropriate, transport records; Breaching the audit-ability. Inability to readily undertake an</p>	<p>implement an enterprise resource planning (ERP);  develop training and prepare instructions for the use of the software;  allow cross checks of information.</p>	



	<p>audit due to the way in which the applicant's accounting system is structured</p> <p>Complex management system offers possibilities to cover-up illegal transactions.</p> <p>No historical data available.</p>		
--	---	--	--

2.2. Audit trail ([Subsection 3.1 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Audit trail	<p>The absence of an adequate audit trail mitigates against an efficient and effective audit based customs control.</p> <p>Lack of control over the system's security and access.</p>	<p>consultation with the customs authorities prior to the introduction of new customs accounting systems to ensure they are compatible with customs requirements;</p> <p>testing and assuring the existence of the audit trail during the pre-audit phase.</p>	<p><a href="#">SAQ 3.1</a></p> <p>ISO 9001:2015, section 6</p>

2.3. Logistic system that distinguishes Union and non-Union goods

Indicator	Risk description	Possible solutions	References
Mix Union and non- Union goods	<p>Lack of logistical system which distinguishes between Union and non-Union goods.</p> <p>Substitution of non- Union goods</p>	<p>internal control procedures</p> <p>data entry integrity checks to verify if the data entries are correct</p>	<p><a href="#">SAQ 3.2.2</a></p>

2.4. Internal control system ([Subsection 3.3 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Internal control procedures	<p>Inadequate control within the applicant over the business processes.</p> <p>No/weak internal control</p>	<p>appointment of a responsible person for quality in charge of procedures and internal controls of the company;</p> <p>make each head of department fully aware of internal controls of their own department;</p>	<p><a href="#">SAQ 3.3</a></p> <p>ISO 9001:2015, , sections 5, 6, 7,,and 8</p>

	<p>procedures offer possibilities for fraud, unauthorised or illegal activities.</p> <p>Incorrect and/or incomplete recording of transactions in the accounting system.</p> <p>Incorrect and or incomplete information in customs declarations and other statements to customs.</p>	<p>record the dates of internal controls or audits and correct identified weakness through corrective actions;</p> <p>notify the customs authorities if fraud, unauthorised or illegal activities are discovered;</p> <p>make the relevant internal control procedures available to the personnel concerned;</p> <p>create a folder/a file in which each type of goods is linked with its own related customs information (tariff code, customs duty rates, origin and customs procedure) depending on the concerned volume of goods;</p> <p>appointment of responsible person(s) for managing and updating the customs regulations applicable (inventory of regulations): i.e. update data in the enterprise resource planning (ERP), clearance or accounting, software;</p> <p>Inform and educate staff regarding inaccuracies and how one can prevent them from happening.</p> <p>Having procedures for recording and correcting errors and transactions in place</p>	
--	---	--	--

2.5. Flow of goods ([Subsection 3.4 from SAQ](#))

Indicator	Risk description	Possible solutions	References
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.	<p>Information of relevant staff and submission of declaration as scheduled;</p> <p>records of stock movements;</p> <p>regular stock reconciliations;</p> <p>arrangements for investigating stock discrepancies;</p> <p>being able to distinguish in the computer system whether goods are cleared or are still subject to duties and taxes.</p>	<p><a href="#">SAQ - 3.4</a></p> <p>ISO 9001:2015, section 6</p>
Incoming flow of goods	Lack of reconciliation between goods ordered, goods received and entries into accounting records.	<p>records of incoming goods;</p> <p>reconciliation between purchase orders and goods received;</p> <p>arrangements for returning/rejecting goods, for accounting and reporting short and over shipments and for identifying and amending incorrect entries in the stock record;</p> <p>formalisation of procedures for import;</p> <p>perform regular inventories;</p>	

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

		perform punctual consistency check of input / output of goods; secure storage areas (special shell protection, special access routines) to fight against the substitution of goods.	
Storage	Lack of control over stock movements.	clear assignment of storage areas; regular stock-taking procedures; secure storage areas to protect against the substitution of goods.	<a href="#">SAQ - 3.4</a> ISO 9001:2015, section 6
Production	Lack of control over stock used in the manufacturing process.	monitoring and management control over the rate of yield; controls over variations, waste, by-products and losses; secure storage areas to fight against the substitution of goods.	<a href="#">SAQ - 3.4</a> ISO 9001:2015, section 6
Outgoing flow of goods Delivery from warehouse and shipment and transfer of goods	Lack of reconciliation between stock records and entries to the accounting records.	persons are appointed to authorise/oversee the sale/release process; formalisation of procedures for export; checks prior to release to compare the release order with the goods to be loaded; arrangements for dealing with irregularities, short shipments and variations; standard procedures for dealing with returned goods – inspection and recording; check the discharge of declaration in case of with custom procedures with economic impact.	<a href="#">SAQ - 3.4</a> ISO 9001:2015, sections 6, and 7

2.6. Customs routines ([Subsection 3.5 from SAQ](#))

Indicator	Risk description	Possible solutions	References
General	Ineligible use of the routines. Incomplete and incorrect customs declarations and incomplete and incorrect information about other customs related activities.  The use of incorrect or outdated standing data, such as article numbers and tariff codes: - Incorrect classification of the	implement formal procedures to manage/follow each customs activity and formalise specific clients (classification of goods, origin, value, etc.). These procedures are intended to ensure the continuity of customs department in case of the absence of assigned staff; use Binding Tariff Information (BTI) that set the duties and import taxes and applicable regulations (sanitary, technical, trade policy measures, etc.); use BOI which provides the administration's advice on: the origin of the product you want to import or export, especially when the various stages of production have taken place in different countries; whether or not to receive preferential treatment under a convention or international agreement;	<a href="#">SAQ - 3.5</a> ISO 9001:2015, section 6

	<p>goods - incorrect tariff code - Incorrect customs value.</p> <p>Lack of routines for informing customs authorities about identified irregularities in compliance with customs requirements.</p> <p>The Binding Tariff Information (BTI) is now also binding for the holder of the BTI. The customs declaration has to refer to the BTI (Article 33 UCC).</p>	<p>setting up formal procedures for the determination and the declaration of customs value (valuation method, calculation, boxes of the declaration to fulfil and documents to produce); implement procedures for notification of any irregularities to customs authorities.</p>	
Representation through third parties	Lack of control	<p>routines to check third parties work (e. g. on customs declarations) and identifying irregularities or violations be representatives should be implemented. It is not sufficient to rely completely on outsourced services; verification of the competence of the representative used; if the responsibility for completing customs declarations is outsourced: specific contractual provisions to control customs data a specific procedure to transmit the data which are necessary for the declarant to determine the tariff (i.e. technical specifications of goods, samples, etc.) if externalisation of the exportation of goods by an approved exporter, the outsourcing can be committed to a customs agent allowed to act as the authorised representative, as long as the agent is in a position to prove the originating status of the goods." implement formal procedures of internal control in order to verify the accuracy of customs data used.</p>	
Licences for import and/or export	Ineligible use of goods	<p>standard procedures to record licences; regular internal controls of the licences validity and registration; segregation of duties between registration and internal controls;</p>	

connected to commercial policy measures or to trade in agricultural goods		standards for reporting irregularities; procedures to ensure the use of goods are consistent with the licence.	
---	--	---	--

2.7 Non-fiscal requirements ([Subsection 3.5.4 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Non-fiscal aspects	Ineligible use of goods falling under prohibitions and restrictions or commercial policy measures.	procedures for handling of goods with non-fiscal aspects; appropriate routines and procedures should be established: to distinguish goods subject to non-fiscal requirements and other goods; to check if the operations are carried out in accordance with current (non-fiscal) legislation; to handle goods subject to restrictions/prohibitions/embargo, including dual-use goods; to handle licenses as per the individual requirements. - awareness training/education for staff dealing with goods with non-fiscal aspects.	<a href="#">SAQ – 3.5.4</a>

2.8 Procedures as regards back-up, recovery and fall-back and archival options ([Subsection 3.6 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Requirements for record keeping /archiving	Inability to readily undertake an audit due to the loss of information or bad archiving. Lack of back-up routines. Lack of satisfactory procedures for the archiving of the applicant's records and information.	the presentation of an ISO 27001 certificate demonstrates high standards in IT security; procedures for back-up, recovery and data protection against damage or loss; contingency plans to cover systems disruption/failure; procedures for testing back-up and recovery; save the customs archives and commercial documents in secure premises; have a classification scheme; adhere to archive legal deadlines.	ISO 9001:2015, section 6 ISO 27001:2013 ISO norms for standards in the IT security

	Deliberate destruction or loss of relevant information	Backups should be done daily, on either incremental or full basis. Full backups should be done at least once a week. Minimum of three latest consecutive backups should be available at all times. Backups are preferably done remotely through an electronically secure method on a storage facility located at least 300 meters away. Encryption key should also be backed up and stored away from the storage facility.	
--	--	--	--

2.9 Information security – protection of computer systems ([Subsection 3.7 from SAQ](#))

Indicator	Risk description	Possible solutions	References
General	Unauthorised access and/or intrusion to the economic operator's computer systems and or programs.	<p>IT security policy, procedures and standards should be in place and available to staff;</p> <p>the presentation of an ISO 27001 certificate demonstrates high standards in IT security;</p> <p>information security policy;</p> <p>information security officer;</p> <p>- information security assessment or identifying issues relating to IT risk;</p> <p>procedures for granting access rights to authorised persons; access rights are to be withdrawn immediately on transfer of duty or termination of employment.</p> <p>-access to data on need to know basis.</p> <p>using encryption software where appropriate;</p> <p>firewalls;</p> <p>anti-virus protection;</p> <p>password protection on all PC Stations and possibly on important programmes</p> <p>If employees leave their workplace the computer should always secured via keyword</p> <p>Password should be made out of at least eight characters being a mixture of two or more of upper and lower letters, numbers and other characters. The longer the password, the stronger it is. Usernames and passwords should never be shared.</p>	<p><a href="#">SAQ - 3.7</a> ISO 27001:2013</p>

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

		testing against unauthorised access; limit access to server rooms to authorised persons; perform tests intrusion at regular intervals; intrusion tests are to be recorded. implement procedures for dealing with incidents.	
General	Deliberate destruction or loss of relevant information.	contingency plan for loss of data; back-up routines for system disruption/failure; procedures for removing access right; procedures to inhibit the use personal consumer ware like pen drives, CD's, DVD's and any other personal electronic peripherals. restrict the use of internet to sites that are only appropriate to business activities	ISO 28001:2007, section A 3 ISO 27001:2013

2.10 Information security – documentation security ([Subsection 3.8 from SAQ](#))

Indicator	Risk description	Possible solutions	References
General	Misuse of the economic operator's information system to endanger the supply chain.  Deliberate destruction or loss of relevant information.	the presentation of an ISO 27001 certificate demonstrates high standards in IT security; procedures for authorised access to documents; filing and secure storage of documents; procedures for dealing with incidents and taking remedial action; recording and back-up of documents, including scanning; contingency plan to deal with losses; possibility to use encryption software if needed; commercial agents to be aware of security measures while travelling (never consult sensitive documents in transport); set up access levels to strategic information according to different categories of personnel; handle discarded computers in a secure manner; arrangements with business partners for protecting/use of documentation.	<a href="#">SAQ - 3.8</a> ISO 28001:2007, section A 4 ISO 27001:2013
Security and safety requirements	Misuse of the economic operator's information system to endanger the supply chain.	requirements to protect data included in contracts; procedures to control and audit the requirements in contracts.	

imposed on others	Deliberate destruction or loss of relevant information.		
-------------------	---	--	--

3. Financial solvency ([Section 4 from SAQ](#))  
Criterion: Proven financial solvency (Articles 39 (c) UCC and 26 UCC IA)

3.1. Proven solvency

Indicator	Risk description	Possible solutions	References
Insolvency/failure to meet financial commitments	Financial vulnerability that can lead to future non-compliant behaviour.	examine the financial statements and financial movements of the applicant to analyse the applicant's ability to pay their legal debts. In most cases the applicant's bank will be able to report on the financial solvency of the applicant; internal monitoring procedures to prevent financial threats.	

4. Security and safety requirements ([Section 6 from SAQ](#))  
Criterion: Appropriate security and safety standards (Articles 39 (e) UCC and 28 UCC IA)

4.1 Security assessment conducted by the economic operator (self-assessment)

Indicator	Risk description	Possible solutions	References
Self-assessment	Inadequate security and safety awareness in all relevant departments of the company	risk and threat self-assessment is carried out, regularly reviewed/updated and documented; identify precisely security and safety risks arising from activities of the company; assess the risks related to security and safety (% of probability or risk level: low/medium/high); make sure all the relevant risks are covered by preventive and or corrective measures.	<a href="#">SAQ - 6.1.2</a> ISO 28001:2007, section A.4 ISPS Code Attachment 6-B 'Checklist for known consignors' airfreight-security



**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

			criteria for Regulated Agent / Known Consignor
Security management and internal organisation	Inadequate coordination about security and safety within the applicant's company.	appointment of responsible person with sufficient authority to coordinate and implement appropriate security measures in all relevant departments of the company; implement security policy including formal procedures to manage/follow each logistical activity from a security and safety point view; - implement procedures to ensure security and safety of goods in cases of holidays or other types of absences of assigned staff;	<a href="#">SAQ - 6.1.4</a> ISO 28001:2007, section A.3 ISO 9001:2015, section 5 ISPS Code
Internal control procedures	Inadequate control within the applicant's company over security and safety issues	implement internal control procedures on security & safety procedures/issues;  procedures for recording and investigating security incidents, including reviewing the risk and threat assessment and taking remedial action where appropriate.	<a href="#">SAQ - 6.1.7</a> ISO 28001:2007, section A.3, A.4 ISPS Code
Internal control procedures	Inadequate control within the applicant's company over security and safety issues	registration can be done in a file containing for example date, observed anomaly, name of the person who has detected the anomaly, countermeasure, signature of the responsible person; make the register of security and safety incidents available to employees of the company.	ISO 28001:2007, section A.3, A.4 ISPS Code
Security and safety requirements specific to goods	Tampering of goods	implement a goods tracking system; special packaging or storage requirements for hazardous goods.	ISPS Code

4.2. Entry and access to premises ([Subsection 6.3 from SAQ](#))

Indicator	Risk description	Possible solutions	References
-----------	------------------	--------------------	------------

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

<p>Routines for access or entry of vehicles, persons and goods</p>	<p>Unauthorized access or entry of vehicles, persons or goods to the premises and/or close to the loading and shipping area.</p>	<p>the number of vehicles with access to the premises should be as limited as possible;  for that reason parking for staff should be preferably outside the security ring;  in addition it can be implemented, if possible, that trucks are waiting before and after loading in a separate area outside the security area. Only signed in trucks will get access to the loading area on demand for the time of the loading;  the usage of badges is reasonable. The badges should have a photo on it. If there is no photo on it the badges should at least indicate the name of the operator or the premises they are valid for (risk for misuse in case they are lost).  The use of badges needs to be supervised by a responsible person. Visitors should have temporary identification badges and be accompanied at all time.  Data on all entries including names of visitors/drivers, arrival/departure time and attendant should be recorded and stored in appropriate form (e.g. logbook, IT system) and are enumerated.  Badges not to be used twice in a row to avoid passing the badge to a companion;  access control with codes: routines for changing the code regularly;  badges and codes should only be valid during the working hours of the employee;  Standardised procedures for the return of all access authorisations;  Visitors should be met and supervised by the business to prevent any unauthorised activities;  Identification badges for visitors have to be worn visible;  Speak to unknown persons;  Corporate clothing to recognise unknown persons;  In case of temporary work (i.e. Maintenance work) a list of authorised workers of the outsourced company.</p>	<p><a href="#">SAQ – 6.3</a>  ISO 28001:2007,  section A.3  ISPS Code</p>
<p>Standard operating procedures in case of intrusion</p>	<p>No proper action if intrusion has been discovered.</p>	<p>implement procedures for cases of intrusion or unauthorised entry;  conduct intrusion tests and record the test results and, if necessary, implement corrective actions;  use of incident report or other appropriate form to record incidents and action taken;</p>	<p>ISO 28001:2007,  section A.3  ISPS Code</p>

		implement remedial measures as a result of incidents related to unauthorised entry.	
--	--	---	--

4.3. Physical security ([Subsection 6.2 form SAQ](#))

Indicator	Risk description	Possible solutions	References
External boundaries of premises	Inadequate protection of the premises against external intrusion.	where appropriate secure perimeter fencing is in place with regular inspections to check integrity and damage and planned maintenance and repairs; where appropriate controlled areas for authorised personnel only are adequately signed and controlled; Irregular patrols of the security staff.	<a href="#">SAQ – 6.2</a> ISO 28001:2007, section A.3 ISPS Code
Gates and gateways	Existence of gates or gateways which are not monitored.	all gates or gateways in use should be secured by using of appropriate measures, i.e. CCTV and/or entry control system (lightening, beamers, etc.); CCTV is only useful when the recordings are evaluable and can lead to contemporary reactions if appropriate, implement procedures to ensure the protection of access points.	ISO 28001:2007, section A.3 ISPS Code
Locking devices	Inadequate locking devices for external and internal doors, windows, gates and fences.	instruction/procedure on use of keys is in place and available for staff concerned; only authorised personnel have access to keys for locked buildings, sites, rooms, secure areas, filing cabinets, safes, vehicles, machinery and air cargo; conducting periodic inventories of locks and keys; log attempts of unauthorised access and check this information on a regular basis; Windows and doors should be locked when nobody is working in the concerned room / office	<a href="#">SAQ - 6.2.4</a> ISO 28001:2007, section A.3
Lighting	Inadequate lighting for external and internal doors, windows, gates, fences and parking areas	adequate lighting inside and outside; where appropriate the use of back-up generators or alternative power supplies to ensure constant lighting during any disruption to local power supplies; plans in place to maintain and repair equipment.	<a href="#">SAQ - 6.2.4</a>

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

Procedures for access to keys	Lack of adequate procedures for access to keys. Unauthorised access to keys.	a key access control procedure should be implemented; keys should be handed out only after registration and be given back immediately after usage. The return of the key has to be registered, too.	ISO 28001:2007, section A.3.3
Internal physical security measures	Inappropriate access to internal sections of the premises.	implement a process to distinguish the different categories of employees in the premises (i.e. jackets, badges); access controlled and personalised according to employees' position.	ISO 28001:2007, section A.3, A.4 ISPS Code
Parking of private vehicles	Lack of adequate procedures for parking of private vehicles. Inadequate protection of the premises against external intrusion.	the number of vehicles with access to the premises should be as limited as possible; specially designated car park areas for visitors and staff are remote from any cargo handling or storage areas; identification of risks and threats of unauthorised entry of private vehicles to protected areas; defined rules/procedure for entry of private vehicles in the applicant's premises; in case of non-separate parking area for visitors and employees, cars of the visitors should have an identification	
Maintenance external boundaries and buildings	Inadequate protection of the premises against external intrusion as a result of inappropriate maintenance.	regular maintenance of the external boundaries of the premises and the buildings each time an anomaly is detected.	ISO 28001:2007, section A.3

4.4. Cargo units ([Subsection 6.4 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Routines for access to cargo units	Lack of adequate procedures for access to cargo units. Unauthorised access to cargo units.	identification of risks and threats of unauthorized access to shipping areas, loading docks and cargo areas; implement procedures governing access to shipping areas, loading docks and cargo areas; cargo units are placed in a secure area (e.g. a fenced area, an area with video surveillance or monitored by security personnel) or other measures are taken to assure the integrity of the cargo unit; access to the area where cargo units are held is restricted to authorised persons;	<a href="#">SAQ - 6.4.1</a> ISO 28001:2007, section A.3 ISPS Code

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

		- share planning between the transport department and the goods reception desk.	
Routines for ensuring the integrity of cargo units	Tampering with cargo units.	procedures for monitoring & checking the integrity of cargo units; procedures for recording, investigating and taking remedial action when unauthorised access or tampering has been discovered; where appropriate supervision by CCTV.	<a href="#">SAQ -6.4.2</a> ISO 28001:2007, section A.3.3 ISPS Code
Use of seals	Tampering with cargo units.	use of container seals that are compliant with ISO/PAS 17712 or other appropriate type of system ensuring the integrity of cargo during transportation; seals stored in a secure location; register of seals is maintained (including used ones); regular reconciliation between register and seals held; - where applicable make arrangements with business partners to check the seals (integrity and numbers) at arrival.	<a href="#">SAQ - 6.4.3</a> ISO/PAS 17712
Procedures for inspecting the structure of the cargo unit including ownership of cargo units	Use of hidden places in cargo units for smuggling purposes.  To have incomplete control of the cargo units.	procedures to examine the integrity of the cargo unit prior to loading; where appropriate use of seven point inspection process (front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage prior to loading); other kinds of inspections depending on the kind of cargo unit.	<a href="#">SAQ - 6.4.4</a> ; <a href="#">SAQ - 6.4.5</a> ISO 28001:2007, section A.3
Maintenance of cargo units	Tampering with cargo units.	regular programme of routine maintenance; if maintenance is carried out by a third party, procedures to examine the integrity of the cargo unit after that.	<a href="#">SAQ - 6.4.5</a> ISO 28001:2007, section A.3
Standard operating procedures in case of	No proper action if unauthorised access or tampering has been discovered.	appropriate procedures laid down on what measures should be taken when an unauthorised access or tampering is discovered.	ISO 28001:2007, section A.3

intrusion and/or tampering with cargo units		
---	--	--

4.5 Logistical processes ([Subsection 6.5 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Active means of transport entering/leaving the customs territory of the Community	Lack of control over the transport of goods.	use of track and trace technology can show unusual stops or delays which could have affected the security of the goods; special procedures for the selection of carriers/freight forwarders; - make arrangements with business partners to check the seals (integrity and numbers) when the goods arrive at their premises.	<a href="#">SAQ - 6.5</a>

4.6 Incoming goods ([Subsection 6.6 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Routines for checking incoming transport	Introduction, exchange or loss of received goods.  Uncontrolled incoming goods which may pose a security or safety risk.	maintain a schedule of expected arrivals; procedures for handling unexpected arrivals; perform consistency checks between incoming goods and entries in the logistics systems; procedures for testing the integrity of the means of transport.	<a href="#">SAQ - 6.6.1</a> ISO 9001:2015, section 6.2.2 ISO 28001:2007, section A.3
Routines for verifying security measures imposed on others	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	procedures for ensuring staff are aware of security requirements; management/supervision checks to ensure the security requirements are complied with.	<a href="#">SAQ - 6.6.2</a> ISO 28001:2007, section A.3
Supervision for the	Lack of control on receipt of goods which may pose a	personnel assigned to receive the driver on arrival and supervise the unloading of goods;	<a href="#">SAQ - 6.6.3</a> ISO 28001:2007,

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

receipt of goods	security or safety risk. Introduction, exchange or loss of received goods.	use pre-arrival information; procedures to ensure assigned staff are present at all times and goods are not left unsupervised perform consistency checks between incoming goods and the transport documents; for the transportation of secure air cargo/air mail from a known consignor have appropriate systems and procedures in place for checking the haulier declaration and identification of the haulier.	section A.3
Sealing of incoming goods	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods	procedures for checking the integrity of seals and the correspondence of the seal number with the number in the documents; appointment of designated authorised person.	<a href="#">SAQ - 6.6.3</a> ISO 28001:2007, section A.3 ISO/PAS 17712
Administrative and physical procedures for the receipt of goods	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods	checks to compare the goods with the accompanying transport and customs documents, picking lists and purchase orders; checks on completeness by weighing, counting, and tallying and checks on the uniform marking of goods; updating stock records as soon as possible on arrival; place goods that pose an anomaly in a specific and secure area and create a process to manage these goods.	<a href="#">SAQ - 6.6.4</a> , <a href="#">6.6.5</a> , <a href="#">6.6.6</a> ISO 9001:2015, section. 7
Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	procedures to record and investigate irregularities e.g. short shipments, broken anti-tampering devices including reviewing procedures and taking remedial action.	<a href="#">SAQ - 6.6.7</a>

4.7 Storage of goods ([Subsection 6.7 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Assignment of storage location	Inadequate protection of the storage area against external intrusion	procedures governing access to the area for storage of goods; an area or areas is/are designated for the storage of goods with CCTV surveillance system or other appropriate controls.	<a href="#">SAQ - 6.7.1</a> & <a href="#">6.7.2</a>

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

Goods to be stored outdoors	Manipulation of those goods	need to use adequate lighting and if appropriate CCTV surveillance; integrity of those goods has to be checked and documented before loading; if possible show the destination of those goods at the latest possible stage (for i.e. bar codes instead of plain text indicating destination).	
Internal control procedures	Lack of procedures to ensure security and safety of stored goods. No proper action if discrepancies and/or irregularities are discovered.	procedures for regular stocktaking and recording and investigating any irregularities/discrepancies including reviewing procedures and taking remedial action. Instructions regarding goods notification addressing how and in what way the incoming goods will be checked.	<a href="#">SAQ - 6.7.3</a> ISO 9001:2015, section 2
Separate storage of different goods	Unauthorised substitution of goods and/or tampering with goods.	location of goods is recorded in stock records; where appropriate different goods e. g. goods falling under restrictions or prohibitions, community/non community goods, hazardous goods, high value goods, overseas/domestic goods, air cargo are stored separately.	<a href="#">SAQ - 6.7.4</a> TAPA (Technology Asset Protection Association) Certificate
Additional security and safety measures for access to goods	Unauthorised access to the goods.	authorised access to the storage area only for designated staff; visitors and third parties should have temporary identification badges and be accompanied at all time; data on all visits including names of visitors/third parties, arrival/departure time and attendant should be recorded and stored in appropriate form (e.g. logbook, IT system); - if own storage area is at another operator premises this area should be secured by regular communication between the operators involved and by visits and controls on spot by the AEO.	<a href="#">SAQ - 6.7.5</a> ISO 28001:2007, section A.3 ISPS Code

4.8 Production of goods ([Subsection 6.8 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Assignment of production location Additional security and	Lack of procedures to ensure security and safety of manufactured goods. Unauthorised access to the goods.	an area is designated for production of goods with appropriate access controls; authorised access to the production area only for designated staff; visitors and third parties have to wear high visibility vests and be accompanied at all times; procedures to ensure safety and security of production processes.	<a href="#">SAQ - 6.8.2</a> ISO 28001:2007, section A.3



**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

safety measures for access to goods			
Internal control procedures	Lack of procedures to ensure security and safety of manufactured goods. Tampering with the goods.	security processes and procedures should be established to assure the integrity of the production process, e.g. authorised access only for designated staff or appropriately authorised persons, supervision and monitoring of the production process by systems and/or personnel.	ISO 28001:2007, section A.3
Packing of products	Incomplete control over the packing of the products. Introduction, exchange or loss of produced goods.	wherever possible products should be packed in a way that tampering is easily to be detected. An example could be the use of special tape with brand names on it. The tape has to be kept under supervision in that case. Another solution is to use tape which cannot be removed residue-free; technological aids to packing integrity may also be used e.g. CCTV surveillance, or weight checking; if possible show the destination of those goods at the latest possible stage (for i.e. bar codes instead of plain text indicating destination).	<a href="#">SAQ - 6.8.3</a>
Quality inspection	Incomplete control over the flow of goods. Introduction, exchange or loss of produced goods.	carry out random security and safety checks of produced goods at each stage of production.	

4.9 Loading of goods ([Subsection 6.9 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Routines for checking outgoing transport	Lack of control of delivery of goods which might pose a security or safety risk.	control the goods loaded (consistency checking / counting / weighing / load order of sales against the information from logistics departments). Check with the logistical system procedures on reception of means of transport are in place; strict access control to the loading area.	<a href="#">SAQ – 6.9.1</a> ISO 28001:2007, section A.3
Routines for verifying security measures	Breach of agreed security arrangements with the risk of delivery of unsafe or insecure goods; delivery of goods	procedures for ensuring staff are aware of customer’s security requirements; management/supervision checks to ensure the security requirements are complied with.	<a href="#">SAQ - 6.9.3</a> ISO 28001:2007, section A.3

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

imposed by others	which is not registered in a logistical system and of which you don't have any control.		
Supervision over loading of goods	Lack of supervision of loading of goods which might pose a security or safety risk.	checks on completeness by weighing, counting, tallying and uniform marking of goods; procedures for announcing drivers before arrival; personnel assigned to receive the driver and supervise the loading of goods; drivers have no unsupervised access to the loading area; procedures to ensure assigned staff are present at all times and goods are not left unsupervised; appointment of responsible person(s) to carry out checks on routines.	<a href="#">SAQ - 6.9.4</a> ISO 28001:2007, section A.3
Sealing of outgoing goods	Sending out goods that are not sealed can lead to introduction, exchange or loss of goods which cannot easily be discovered.	procedures for controlling, applying, checking and recording seals; appointment of designated authorised person; - use of container seals that are compliant with ISO/PAS 17712.	<a href="#">SAQ - 6.9.2</a> ISO 28001:2007, section A.3 ISO/PAS 11712:116 ISO PAS 17712
Administrative processes of the loading of goods	Delivery of goods which is not registered in a logistical system and of which you don't have any control and thus posing a security or safety risk.	checks to compare the goods with the accompanying transport and customs documents, loading/packing lists and sales orders; updating stock records as soon as possible after departure.	<a href="#">SAQ - 6.9.5</a> and <a href="#">6.9.6</a>
Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	procedures to record and investigate irregularities e.g. short shipments, broken anti-tampering devices, customer returns, review procedures and take remedial action.	<a href="#">SAQ - 6.9.7</a> ISO 28001:2007, section A.3

4.10 Security requirements on business partners ([Subsection 6.10 from SAQ](#))

Indicator	Risk description	Possible solutions	Reference
-----------	------------------	--------------------	-----------

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

Identification of business partners	Lack of mechanism for clear identification of the business partners.	<p>procedure in place for identifying regular business partners and unknown clients/customers;</p> <p>procedures to select and manage business partners where the transport is carried out by a third party;</p> <p>implement a procedure to select subcontractors based on a list of regular and irregular subcontractors;</p> <p>subcontractors can be selected on the basis of selection criteria or even of a company specific certification (which can be set up on the base of a certification questionnaire).</p>	
Security requirements imposed on others	Breach of agreed security arrangements with the risk of receiving or delivering unsafe or unsecured goods.	<p>background checks used to select regular business partners e.g. through the use of internet or rating agencies;</p> <p>security requirements (e.g. that all goods must be marked, sealed, packed, labelled in a certain way, subject to X-ray checks) are written into contracts with regular business partners;</p> <p>requirement that contracts will not be further sub-contracted to unknown third parties particularly for the transportation of secure air cargo/air mail;</p> <p>conclusions provided by experts/external auditors, not related to regular business partners, on complying with security requirements;</p> <p>evidence that business partners hold relevant accreditations/certificates to prove they comply with international security standards;</p> <p>procedures for carrying out additional security checks on transactions with unknown or irregular business partners;</p> <p>reporting and investigation of any security incidents involving business partners and recording remedial action taken.</p>	<p><a href="#">SAQ – 6.10</a> ISO 28001:2007, section A.3</p>

4.11 Personnel security ([Subsection 6.11 from SAQ](#))

Indicator	Risk description	Possible solutions	References
Employment policy including	Infiltration of staff that could pose a security risk.	<p>background checks on prospective employees, e.g. previous employment history and references;</p> <p>additional checks on new or existing employees moving to security sensitive</p>	<p><a href="#">SAQ - 6.11.2;</a> <a href="#">SAQ - 6.11.4</a></p>

**Annex 2**  
**to TAXUD/B2/047/2011- REV6**

for temporary personnel		posts e.g. police checks on unspent convictions; requirements on staff to disclose other employment, police cautions/bail, pending court proceedings, or convictions; periodic background checks/reinvestigations for current personnel; removal of computer access, return of security pass, keys and/or badge when staff leave or are dismissed; checks on temporary staff applied at the same standard as permanent staff; contracts with employment agencies detail level of security checks required; procedures to ensure employment agencies comply with those standards.	ISO 28001:2007, section A.3
Level of safety and security awareness of personnel	Lack of proper knowledge on security procedures related to different process (incoming goods, loading, unloading, etc.) with the consequence of accepting/loading/unloading unsafe or insecure goods.	staff awareness on security measures/arrangements related to different process (incoming goods, loading, unloading, etc.); set up a register for recording security and safety anomalies and discuss this with staff on a regular basis; procedures in place for employees to identify and report suspicious incidents; pamphlets on security and safety issues can be displayed in specific areas and communicated via a notice-board; display the security & safety rules in the relevant areas (loading/unloading etc.). The signs must be visible internally (in the sites) and externally (places dedicated to the drivers, temporaries, various partners).	ISO/28001:2007, section A.3
Security and Safety training	Lack of mechanisms for training employees on safety and security requirements and, consequently, inadequate awareness of security requirements.	persons responsible for identifying training needs, ensuring delivery and keeping training records; training employees to recognise potential internal threats to security, detection of intrusion/tampering and preventing unauthorised access to secure premises, goods, vehicles, automated systems, seals and records; conducting tests with “unsafe” goods or occasions; security and safety training can be part of industrial safety training to outreach all staff; Security and Safety trainings have to be documented and updated regularly based on happened situations in the company (e.g. every year); New staff should be trained intensively due to their lack of knowledge and awareness.	<a href="#">SAQ - 6.11.3</a> ISO 28001:2007, section A.3

4.12 External services ([Subsection 6.12 from SAQ](#))

Indicator	Risk description	Possible solutions	References
External services used for various areas, i.e. packing of products, security, etc.,	Infiltration of staff that could pose a security risk.  Incomplete control over the flow of goods	security requirements e.g. identity checks on employees, restricted access controls are written into contractual agreements; monitoring compliance with these requirements; use of different badges for external staff; restricted or controlled access to computer systems; supervise external services where appropriate; establish security arrangements and or auditing procedures to ensure the integrity of the goods; In case of temporary work (i.e. maintenance work) a list of authorised workers of the outsourced company.	<a href="#">SAQ 6.12</a> ISO 28001:2007, section A.3

Annex 3

**Security Declaration<sup>1</sup>**  
**for Authorised Economic Operators**  
**AEO**

Name (Company) \_\_\_\_\_  
Street Address \_\_\_\_\_  
City \_\_\_\_\_  
Country \_\_\_\_\_  
Postal Code \_\_\_\_\_  
Phone \_\_\_\_\_  
e-Mail \_\_\_\_\_

I hereby declare that:

- goods, which are produced, stored, forwarded or carried by order of Authorised Economic Operators (AEO), which are delivered to AEO or which are taken for delivery from AEO
  - are produced, stored, prepared and loaded in secure business premises and secure loading and shipping areas
  - are protected against unauthorized interference during production, storage, preparation, loading and transport
- reliable staff is employed for the production, storage, preparation, loading and transport of these goods
- business partners who are acting on my behalf are informed that they also need to ensure the supply chain security as mentioned above.

Name of Authorised Signatory <sup>2</sup> _____	Company Stamp (where required)
Position _____	
Signature _____	
Date issued _____	

This declaration was issued to:

Name (Company) \_\_\_\_\_  
Street Address \_\_\_\_\_  
City \_\_\_\_\_  
Country \_\_\_\_\_  
Postal Code \_\_\_\_\_

---

<sup>1</sup> Necessary adjustments to the text should be made to take into account the parties' respective business models and roles in the international supply chain.

<sup>2</sup> Authorised Signatory registered at the Commercial Register

### **Examples of information to be shared with customs authorities**

In application of Article 23 (2) UCC, *"the holder of the decision shall inform the customs authorities without delay of any factor arising after the decision was taken, which may influence its continuation or content"*.

This document aims to help AEOs in identifying some of the situations, which may have both an impact on the content of the AEO authorisation and / or on the criteria they have to fulfil according to Article 39 UCC.

**This annex is not a comprehensive check-list, but an indicative tool to help operators in their relation with customs authorities for the management of their AEO authorisation(s).**

If the economic operator considers a fact not listed below that may have an impact on its AEO authorisation, customs is to be informed. Furthermore informing the competent customs authorities does not relieve the economic operator from any other reporting duties.

The scope of information to be notified to customs authorities depends on the type of AEO authorisation held: AEOC or AEOS.

Indeed, AEOC do not have to fulfil the requirements laid down in Article 39 (e) UCC and Article 28 UCC IA, while AEOS are not concerned by the requirements of Article 39 (d) UCC and Article 27 UCC IA.

### **Examples of information to be transmitted to Customs authorities**

#### **General information**

Any changes related to the:

- Company name
- Legal status
- Merger or demerger
- Place of establishment
- Correspondence address (if different from the address of establishment)
- Correspondence address for MRA communications (if different from the address of establishment)
- Contact person
- Sale or closure of business
- economic sector of activity and/or role in the supply chain

**Compliance (Article 39 (a) UCC + Article 24 UCC IA)**

- Any serious or repeated infringement of customs legislation, taxation rules or serious criminal offences relating to the economic activity (e.g. being convicted of deception, bribery, corruption) by:

- the applicant,
- the person in charge of the applicant company or exercising control over its management,
- the employee in charge of the applicant's customs matters

- Change in the company management or structure, for instance: new owner, new person in charge of the applicant or controlling its management or new employee(s) in charge of customs matters

- Any pending criminal proceeding linked to an infringement of the customs legislation, taxation rules or criminal offences to the economic activity.

**Satisfactory system of managing commercial  
and transport records (Article 39 (b) UCC + Article 25 UCC IA)**

- Changes or updates of the accounting or logistic systems
- Dysfunction of the accounting system (e.g. loss of accounting data, lack of traceability etc.)
- Accounts not certified by an external auditor
  
- Loss of records
- Dysfunction of cross-checked audits
  
- Loss or destruction of accounting, commercial and transport archives
  
- Loss or destruction of electronic backups of accounting, commercial and transport data
  
- Incapability of distinguishing Union and non-Union goods due to e.g., a crash of the software used
  
- Incapability of managing internal controls
- Discovery of an important irregularity during an internal control
- Corrective measures to correct major irregularities detected
  
- New process to deal with a product requiring licences and authorisations in accordance with commercial policy measures or relating to trade in agricultural products
  
- New location of archives



- Usage of a wrong commodity code
  - Usage of a wrong customs value
  - Processing of goods in temporary storage by accident
  - Any problem in temporary storage or customs warehousing which is related to customs activities
  - Processing of goods under transit procedure by accident
  - Identification of an accumulation of working mistakes
  - Non-observance of prohibitions or restrictions
- 
- Intrusion detected into IT systems
  - Major dysfunction of IT security measures
  - Major breakdown of the IT system

- New process to deal with products covered by prohibitions or restrictions
---

<b>Financial Solvency (Article 39 (c) UCC + Article 26 UCC IA)</b>
--

- AEO subject to any insolvency proceedings
  
- Payment incidents with regard to customs duties or other duties and taxation rules related to import or export of goods

- Any negative change in the financial standing including negative net assets that cannot be recovered
- Loss of major clients
- Loss of major markets
- Loss of commercial franchising, concessions, marketing and/or commodity trading licenses
- External auditor negative reports/audit finding in annual financial audits

<b>Practical standards of competence or professional qualifications (Article 39 (d) UCC + Article 27 UCC IA)</b>
--

- Any changes relating to the person in charge of customs matters
  
- Loss/Acquisition of a quality standard concerning customs matters adopted by an European Standardisation body

- In case of designation of a new employee in charge of customs matters, provision of evidence of relevant training in customs matters
--

--

<b>Security and safety standards (Article 39 (e) UCC + Article 28 UCC IA)</b>
---

- Acquisition of new premises / new buildings / move
  
- New security plan; new process or new security measures to access offices, shipping areas, loading docks, cargo areas
- Any serious security incident (e.g. intrusion of unauthorised persons, burglary etc.) and corrective measures taken to cope with it
  
- Information of a security issue related to the application of internal processes (e.g. 7 points inspection which would reveal a false floor/bottom; unusual repairs etc.)
- Serious incident during transportation of goods
  
- Difficulties with securing business partners
- Detection of fraud or malpractice/misconduct from business partners
  
- Information resulting from background checks on the employee, with negative impact on the security and safety
- Difficulties with securing external service providers
  
- Difficulties to implement an awareness programme scheduled and presented to customs during a previous audit
  
- Changes regarding the contact person for security and safety matters, e.g. new contact person, changes in name etc.

**Related topics**

**- Which changes could have an impact on several criteria?**

Some changes may have an impact on the respect of multiple criteria of the authorisation(s). In that case, it is strongly recommended that AEOs inform the competent customs authorities well in advance to anticipate this situation and to determine the best solutions to cope with it.

**- Which information can have an impact on the conditions of the initial acceptance of the application?**

Sometimes an AEO will change its economic activity after being authorised as an AEO, for instance by stopping its operations related to customs matters or by stopping any activity

related to the international supply chain (for instance when the AEO operates exclusively on national/European level).

It is expected from AEOs to inform their ICA in case of such changes in order to find the most appropriate solution to cover each particular situation.

**- How can an AEO monitor its authorisation internally to ensure not to miss any important information to be notified?**

The AEO contact person will play an important role to monitor the ongoing fulfilment of AEO criteria in the company. According to the size of the company, different organisations can be implemented to ensure a relevant monitoring of the AEO authorisation (e.g. regular meetings, regular updates of procedures with the relevant divisions of the company, use of an Electronic Document Management System etc.).

**- Who has to be notified of these changes?**

Each competent customs authority can determine the best procedures to follow (local contact point, regional contact point, national contact point) according to its size and organisation. It is strongly recommended that competent customs authorities provide a contact point within the Customs administration to whom any information from operators should be notified.

When the AEO authorisation covers premises in more than one Member State,

**- How does the information have to be transmitted to the competent customs authorities?**

The competent customs authorities should determine the accepted ways of transmission of this information and should inform the AEO of the contact point designated within the administration. In order to communicate these changes, the competent customs authorities can recommend the best way(s) to proceed (e.g. email, formal letters or a template).

**- Impact of these changes on the monitoring of the authorisation by the ICA:**

- According to the information transmitted by the AEO, the ICA will determine whether it is necessary or not to take any specific action such as to launch a monitoring audit or a re-assessment audit.
- The ICA can also consider that no further action has to be undertaken in case the changes are considered as minor.