CUSTOMS AEO VALIDATOR GUIDE

Contents

CUSTOMS AEO VALIDATOR GUIDE

Purpose:

The Guide provides practical guidance to assist countries in carrying out AEO validation in a standardised manner sets out the essential elements required, and promotes a common minimum set of competencies of Customs officers tasked with conducting validations.

1. INTRODUCTION

1.1. Background

The SAFE Framework of Standards (FoS) incorporates the AEO concept (Authorized Economic Operator) and provides baseline technical guidance for the implementation of AEO programmes at global level between WCO Members and the international trade community. It is designed to serve as a starting point for national AEO programme implementation and supports the effective application of the standards and information that are outlined in Pillar II (Customs-to-Business Partnerships) and in Annex IV of the SAFE Framework.

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 and mutual respect for each other's roles and responsibilities in this regard. 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.

AEO status is granted to an economic operator that satisfies criteria such as Customs compliance, management of commercial records, financial solvency and appropriate security and safety standards.

AEO validation and the role of an AEO validator therein, is paramount for the AEO concept. The AEO validation procedure, including re-assessment\re-validation and/or monitoring processes is risk based (see also 4 and 5.2.).

The aim of the validation procedure is to verify that the applicant meets, and the AEO continues to meet, the requirements of its scope of authorization. The economic operator that receives an AEO authorization is considered a trusted economic operator for Customs (and, where applicable, for other partner government agencies also), and receives operational benefits. Furthermore by relying on the compliance of the AEO, Customs improve their risk management as well and can use their resources better.

This AEO Validator Guide will provide a set of competencies for the long-term application of the AEO process. These core competencies form a "baseline" that should be followed by all parties engaged in this effort.

1.2. The aims of this Guide

The Guide is intended as an aid for administrations in the organisation and carrying out of Customs AEO validation controls. The specific aims are to:

- Create a set of competencies to give the assurance of the competence of Customs validators,;
- Set out essential elements needed to carry out an AEO validation;
- Provide practical guidance to assist AEO validators in carrying out AEO validation in a standardised manner by sharing techniques and expertise;
- Promote a common approach to Customs AEO validation and apply working methods suited to the national, regional and international context.
- Facilitates the efficiency of mutual recognition negotiations and implementations processes.

1.3. Glossary of terms and abbreviations

Authorization: recognition by Customs of AEO status in an AEO programme, based on a structured methodology that includes such processes as review of an applicant's submitted documentation, physical worksite assets and security processes, in order to determine compliance with the core international standards of the SAFE Framework.

Authorized Economic Operator (AEO): an AEO is a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards. AEOs may include, inter alia, manufacturers, importers, exporters, Customs agents/brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors, and freight forwarders.

Economic operator (EO): means a person/entity that, in the course of his business, is involved in activities covered by Customs legislation. The term includes, inter alia, importers, exporters, manufacturers, carriers, etc.

Point (s) of Contact (POC): Economic operator's designated and readily accessible local points of contact or a corporate contact that can arrange immediate access to a local contact for all matters identified as being of compliance and enforcement interest to Customs (cargo bookings, cargo tracking, employee information, etc.);

Quality assurance: regular measurement, comparison with established standards, monitoring of the validation processes and feedback to ensure/assess if the validation process is working correctly and if any improvements are required (see section 6).

Risk assessment /identification: Overall process of risk identification, risk analysis, risk evaluation prioritization and treatment.

Training and development programme: appropriate measures to train validators before beginning their validation work and provide training on a continuing basis in the skills and knowledge appropriate to their duties.

Validation: procedure whereby the applicants, their supply chain(s), and all relevant processes employed by them to reach that status, are subject to full and transparent review by a Customs administration.

Validators: the Customs officials who are responsible for the validation process.

2. FRAMEWORK OF AEO VALIDATION AND AUTHORIZATION PROCEDURES

2.1. The SAFE Framework of Standards References

- SAFE Framework of Standards, Definitions (Annex 1)
- SAFE Framework of Standards, Pillar 2
- SAFE Framework of Standards (Annex IV A to M, SAFE FoS, 2015 version):
    - AEO conditions and requirements
    - Validation and authorization procedures
    - Application and authorization
    - Validation procedure
    - Review and maintenance

2.2. Scope

The AEO authorization process consists of the AEO application process, which includes the formal submission of the application and its acceptance by Customs and is followed by the validation covering the risk-based validation, and the review and maintenance or management of the authorization. It is to be carried out within a time frame defined by Customs together with the private sector, and/or by legislation. The risk-based validation is performed by Customs before the granting of the AEO status. In the context of AEO, the risk-based validation follows the AEO application, and serves to verify whether the applicant fulfills the criteria.

As a result of the risk-based validation the validator must be able to:

- make a judgement about the fulfilment of the conditions for the granting of the authorization;
- identify and evaluate the relevant risks, assess the remaining risks and propose, where necessary, further actions to be undertaken;
- identify elements in the operator's procedures which need closer Customs monitoring, and advise the applicant to improve or strengthen the relevant procedures and controls.

The economic operator must follow up by implementing an action plan that addresses the "actions required" and/or recommendations issued during the validation. This process also includes providing evidence of compliance with the actions required.

Once the authorization has been granted, monitoring may consist of validation based on risk or cause and, where appropriate, random spot checks by Customs; it is done on a continuous basis and could result reassessment or revalidation, including through monitoring of the day-to-day activities of the AEO and, if needed, visits to his premises. It aims at the early detection of any sign of non-compliance, and shall lead to prompt actions in the event that any difficulty or non-compliance is detected.

Re-assessment can be a result of e.g. structural changes in the operations, new legislation or reasonable indication that action must be taken in order to verify whether the economic operator is still compliant with the AEO criteria. In this context, it is clear that monitoring can trigger re-assessment.

The AEO, in order to maintain the level of compliance with the obligations resulting from the authorization, shall inform Customs of any circumstances that may impact its authorization.

2.3. Organisation

The acceptance of the application form, including an assessment of the fulfillment of the requirements, is the responsibility of a nominated person, a specific service or unit within the Customs administration.

The AEO shall appoint a person within his management structure to be responsible for communication with the Customs administration regarding the AEO approval system and the maintenance of standards.

The validation will be carried out by Customs validators. It may be organized using teams of validators led by a team manager. The objective is to put in place an organizational structure that enables the team to carry out their tasks efficiently and effectively. Validators are responsible for executing the validation in the most effective way, correctly applying the appropriate validation procedures and techniques, and ensuring that established criteria are complied with. Team managers are responsible for setting the conditions that allow the validators to achieve this goal and are in charge of building, improving and controlling the validation process.

3 AEO VALIDATOR(S) PROFILE

3.1. Introduction

According to Annex IV in the SAFE FoS, the Customs administration ensures that personnel designated to carry out the validation procedure are trained and qualified.

The team of validators should possess all the core values and skills listed below, including that of professional values, ethics and attitudes.

The team members should have a good, relevant knowledge in order to verify the AEO requirements. For specific areas of a more complex nature, e.g., IT, security and safety, a specialist may be used. This may also be influenced by the size or complexity of the economic operator business activity.

It is highly recommended that officers gain relevant practical experience by accompanying more experienced validators, before having a substantial involvement

in the validation process. In cases of newly developed AEO programme, Customs administrations may seek assistance from other established AEO programmes and/or WCO experts, other compliance/security validation programmes including other international security programmes.

3.2. General competencies of AEO Validators

Customs administrations should ensure that validators have the necessary competencies to undertake an effective AEO validation.

Knowledge Requirements:

- knowledge of Customs legislation, including Customs procedures and regimes and other legislation to be applied by Customs,
- knowledge of Customs simplifications,
- knowledge of the Revised Kyoto Convention, the SAFE Framework of Standards and history of AEO,
- knowledge of national AEO programme,
- knowledge of the legal environment of an economic operator;
- knowledge of risk management principles and techniques
- knowledge of audit and computer-assisted auditing packages and techniques,;
- knowledge of bookkeeping and IT applications for financial accounting and reporting,
- knowledge of information technology including IT security,
- knowledge (basic) of multiple languages where needed,
- knowledge of safety and security programmes from other government or inter- governmental agencies (for example Regulated Agent/Known Consignor, ISPS code, and others),
- knowledge about relevant commercial standards and certifications (for example ISO, TAPA and others)
- knowledge of bilateral or multilateral treaty obligations, local cultures,
- knowledge of the global supply chain and,
- knowledge of Industry's best practices.

Skills Requirements:

- ability to identify and solve problems,
- ability to undertake appropriate technical research,
- ability to liaise with Customs, partner government agencies and economic operators, in a consultative process,
- ability to gather and evaluate evidence (including information from third party experts/service providers or other public authorities),
- ability to present, discuss, and at times defend views effectively through formal, informal, written and spoken communication,
- ability to treat sensitive and confidential information appropriately,

- ability to communicate at multiple levels within the company,
- ability to obtain and interpret relevant economic, environmental, and other information,
- ability to understand the business and to adapt according to the size of the business,
- ability to take an unprejudiced approach with regards to the integrity and trustworthiness of economic operators;
- ability to maintain an open mind when determining the commitment of the economic operator to meet and maintain the AEO criteria throughout its entire organisation, and
- ability to communicate effectively in writing including written reports

Note: The **requirements** can be covered by an individual and/or a team

Professional values, ethics and attitudes

Fundamental principles are:

- Integrity: requires validators to observe the principles of independence, objectivity, standards of professional conduct, and absolute honesty in their work;
- Objectivity: Customs validators must exhibit a high level of professional objectivity in gathering and evaluating information during Customs validations. They must make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments. It is essential that Customs validators are independent and impartial, not only in fact but also in appearance. The validator should declare any prejudicial factors in relation to carrying out a control on a particular operator (e.g., relationship between validators and operator, shareholder, etc.);
- Professional competence and due care: validators must apply the knowledge, skills and experience needed to carry out a Customs validation. Validators must also be aware of their national specific Code of Conduct;
- Confidentiality: Customs validators are required to protect the privacy of individuals and economic operators in official dealings in accordance with national laws;
- Professional behaviour: In every step of the processing of an AEO authorization, validators must be mindful of the image of Customs and the AEO programme they are representing. For this reason, it is important that they act professionally and remain permanently attentive to the operator's questions and/or concerns. They should be able to provide the appropriate response.

3.3. Validation competencies of AEO Validators

The competence, knowledge, skills and experience of a validator is essential. Customs administrations should put in place a structured training programme in order

to achieve the necessary competencies of AEO validators: This requires (in addition to the other competencies):

- Understanding internal control measures
- Accounting and internal control
- Assessing the operator's risks related to the AEO criteria
- Develop a validation plan/control plan
- Perform controls, and
- Complete the validation, draw conclusions and issue a validation report

3.4 External knowledge/development

For Customs validators and their team managers (and the entire Customs administration), it is essential to be aware of what is happening with the external environment in order to adapt and update their professional skills, knowledge and working methods to meet new, rising challenges (e.g., new trends in fraud, new auditing techniques, new legislation, new technologies, how international standards work, global supply chain, etc.).

3.5. Role of AEO Validators

- Prepare for validation: collect, analyse information and assess related risks, prepare validation plan, etc.;
- Coordinate meeting agenda
- Understand the business process;
- Carry out site visits to verify the economic operator´s compliance with the AEO criteria;
- Use of specialist resources as required (e.g., safety and security experts, audit services, intelligence and enforcement experts);
- Obtaining and verifying any supporting documentation;
- Establishing, recording, observing, evaluating and testing the applicant's procedures;
- Use the respective validation report templates
- Completing a report covering the checks carried out and the conclusions drawn;
- Recommending whether the authorization should be granted or refused;
- Being available to advise the company throughout the process; and
- Make the EO aware of the importance to instruct and train employees to inform the Customs administration and, where applicable, other relevant authorities, whenever a compliance and/or security issue arise.

Note: the knowledge, competencies and roles of validators covered under para 3.2 to 3.5 are non-exhaustive and could vary based on national or regional needs and variations. Customs administrations are encouraged to undertake the necessary training and development for their AEO validators, as well as to identify new areas that would be useful for the administration of the country's AEO programme."

4. AEO VALIDATION PROCEDURE

Acceptance procedure for the AEO application

Economic operators are in the best position to prepare their own application for AEO status. However, at the request of the economic operator, Customs administrations may provide assistance for preparing their application.

Upon receipt of the application form, the Customs administration will examine it and decide upon its acceptance or non-acceptance, taking into account the requirements of the relevant provisions and making sure all the information needed to perform a quick check against the acceptance conditions is available.

To assist the applicant in making sure all necessary information is available, a Self-Assessment Questionnaire (SAQ)/AEO Template[1] provided by Customs, and to be submitted with the application, could be useful. Receiving the necessary information from the applicant will make the overall process more efficient afterwards for both customs and the applicant.

In the event that additional information is required, the Customs administration must request it from the applicant as soon as possible, but (if applicable) within the deadline provided for in the legislation or national provisions.

The Customs administration should inform the applicant about the acceptance of the application and the date of acceptance; it should also inform the economic operator in the event of non-acceptance of the application, stating the reasons for non-acceptance.

Risk Analysis

Once an application has been accepted the AEO validation process must adopt a comprehensive approach. This means that the validation must cover all aspects of the business that are involved in the international supply chain, and the AEO criteria must be tested and satisfied against all the Customs activities carried out by the economic operator.

Customs must collect as much relevant information as possible to understand the economic operator´s business in order to identify and analyse potential risk. The analyses of the risk and the weighting of the risk is an initial and continuing process. In order to have comparable results the risk assessment process should be based on a recognised risk analysis model.

There are two aspects to be considered in order to assess the importance of the relevant risk: the likelihood that an event will occur and its potential impact. These two aspects should also be taken into account to determine whether the measures in place are sufficient to cover the identified and relevant risks.

The risk and threat assessment should cover all potential risks including those of relevant government agencies concerning the AEO status, bearing in mind the role played by the economic operator in the supply chain; it should include:

[1] http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/~/media/C5BFD21DF7FF4E18992EA359DD3E4EDB.ashx

- security/safety threats to premises and goods;
- Customs and fiscal risks;
- reliability of information related to Customs operations and logistics in respect of the goods;
- IT security
- reliability of the operator's employees;
- visible audit trail and prevention and detection of fraud and errors;
- security/ safety of business partners in the supply chain.

The AEO validator should be aware of the different risks to be evaluated, in order to execute the validation procedures in a way that ensures the risks are covered. They include inherent risks (for example, counterfeiting) identified through assessing the business environment, control risks not detected by internal control systems, and detection risks not detected by the validation techniques.

According to the risks identified (potential risks) for the specific economic operator the validators have the responsibility to plan and perform the validation in order to verify if he/she is compliant with the criteria.

In this context, Customs' role is also to assess how effectively the economic operator covers the important risks, and whether the measures he takes to cover those risks are adequate.to reduce them to an acceptable level.

An organization that has not implemented any internal control system, or has a system which is shown by evidence to be performing poorly, is by definition at risk.

Within the economic operator's organization, there should be an authorized person or unit (depending on the size and complexity of the company) responsible for carrying out a risk and threat assessment and for putting in place and evaluating the internal controls and other measures.

4.1 General principles of the validation procedure

- **Validation documentation and evidence**

This is the information which allows the validators to reach the conclusions on which their opinion regarding their advice on approval or rejection of the application will be based. It can take several forms: documented procedures and instructions, verbal (e.g interview), observation, physical and analytical.

In all cases the validation evidence must be appropriate (relevant to the validation objective and reliable), credible and sufficient.

To be relevant, evidence should support validation findings and conclusions and should be consistent with the objectives of the validation

To be credible, evidence should be factual, adequate and complete so that a prudent and informed person would be able to understand how the conclusions had been reached

Reliable evidence can be achieved through the use of appropriate validation techniques which should normally be selected in advance, but which may be expanded during the validation work.

The evidence must be fully captured or reflected in the validation report by the validators to substantiate the opinion reached and to allow independent evaluation of the validation carried out.

4.2. Preparation phase

In order to identify the risks and prepare an effective and efficient validation it is vital to get as much information as possible about the economic operator in order to:

- **Understanding the business entity and its organisational structure from the following non-exhaustive list :**
  - ✓ The self-assessment questionnaire (see AEO Template, SAFE Package)
  - ✓ Information provided during the application process
  - ✓ Information from internal Customs sources: internal database (National Risk Database) and filing system;
  - ✓ Information from external sources: other Authorities, via the Internet, companies' annual financial reports, validator's report on internal control, etc., and via communication with Chambers of Commerce and Central Statistics;

- **Understanding trade business organisation through the following non exhaustive elements:**
  - ✓ Partners supply chain
  - ✓ External Service Providers
  - ✓ Logistical processes
  - ✓ Internal procedures

- **Assessing risk factors**
  - ✓ prioritize the risks identified through evaluation of the impact on Customs objectives and the likelihood of the risk materializing;
  - ✓ assess to what extent the operator himself has taken measures to cover identified risks, and in what way the operator has prioritized the different types of risks;
  - ✓ construct a risk profile to provide a comprehensive picture of all significant risks;
  - ✓ reflect on the risk profile constructed.

- **Identify the factors facilitating the process**:

  To take into account, to the extent allowable within a national AEO regime, national and international (security) programmes based on internationally recognised standards such as those from ICAO, IMO, UPUor ISO.

- **Validation work plan**

  It is the responsibility of the validators to plan and perform the validation in order to obtain reasonable assurance as to whether the economic operator is compliant with the established criteria. The validators should determine their work plan according to the risks identified for the specific economic operator. Only Customs administrations have the authority to grant AEO status however conclusions provided by third party experts in the relevant fields related to AEO requirements may be accepted. It is important that visits to the facility be communicated and coordinated in advance with the economic operator´s primary point of contact to ensure, among other things, that appropriate personnel and subject matter experts are available for the validation process. The validation plan should be developed as a result of the risk assessment, and should reflect information about:

  - ✓ the risks of each area, indicating the relevant points/aspects to check;
  - ✓ the management and staff members to interview;
  - ✓ the management and staff members from service providers and/or trading partners to interview;
  - ✓ what, how and when a specific transaction/security test should be done;
  - ✓ validation meeting agenda.

  Customs administrations should have systems and strategies for organizing and performing the validations.

4.3. On-site phase

During this phase, the validators determine whether the controls, procedures and processes identified during the information-gathering phase have actually been implemented, and are operating effectively in the manner described by the applicant. Indeed, a key element of this phase 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.

On-site visit(s) – verifying, as necessary, implementation of the requirements stipulated below (the SAFE Framework of Standards):

- **Arriving at premises**

The Validation starts upon arrival at the economic operator´s premises. If deficiencies are identified upon arrival at the facility, validators should ensure they form part of the validation findings.

- **Meeting:**

All participants at the meeting should introduce themselves and an attendance list can be used and attached to the validation report,

Validators should:

- ✓ establish their credibility and competency at the start of the meeting,
- ✓ explain the AEO-concept and benefits, when applicable
- ✓ provide the EO with an overview on how the Validation meeting/ visit will be conducted,
- ✓ lead the meeting to ensure that it is conducted in an organised manner,
- ✓ be flexible with the times established for the visit/ meeting, For example, take into consideration the EO's working operation when coordinating meeting breaks and conducting the walk-through of the facility,
- ✓ provide the EO with Customs and AEO program updates,
- ✓ explain how observations, recommendations and/or actions required will be communicated when deficiencies are found during the meeting/ visit,
- ✓ explain how best practices will be communicated when observed during the meeting/ visit,
- ✓ explain how there will be a meeting/ visit close-out that will reiterate what has been observed and communicated during meeting/ visit (recommendations, actions required, best practices, etc.),
- ✓ explain that a validation report will be generated that will include the meeting/ visit findings,
- ✓ provide timelines on when the report will be generated and what is the expected timeframe for the EO to submit their validation report response;
- ✓ explain during the close-out meetings to the EO the validation findings and inform them that they do not have to wait until the formal validation report is generated in order to start a corrective action for addressing deficiencies if found during the meeting/ visit,
- ✓ inform the EO, that if a corrective action to address a deficiency is implemented before the validation report is completed, the validators should be informed, and
- ✓ provide specific information that is relevant to secure business partners and to include it in the validation report to show the business partners willingness to participate in the AEO programme;

4.3.1 Conducting the Meeting

Validators should:

- ✓ conduct the meeting and handle themselves in professional manner,

- ✓ emphasize that the principal goal of the validation is to ensure that the EO is complying with the AEO program's criteria for certification,

- ✓ emphasize the validation meeting is also a forum that the Validation Team and EO can build a stronger partnership by discussing trade operation strategies,

supply chain security issues, sharing best practices, and cooperatively developing solutions to address potential vulnerabilities,

- ✓ emphasize that AEO programs are voluntary, and delivered in partnership with the EO with an objective to improve Customs' compliance and supply chain security, and

- ✓ not insist that the meeting is conducted only one particular way. Often the culture of the meeting can take unforeseen turns and it is imperative that validators) recognize the need for flexibility. (For example, if the CEO of the company wants to provide validators with a presentation about an operation, validators should allow for that and use the opportunity to gather information relevant to requirements within the established AEO criteria).

4.3.2 Validation

The scope of the validation is to evaluate the effectiveness of the procedures and measures taken by the EO in order to cover the relevant risks.

It should focus on the risks related to all AEO requirements in order to ensure that any remaining risk is acceptable to the Customs administration.

It is critical that EO upper management is committed to the validation process which ensures that the applicant truly supports the AEO programme, including the necessary measures to be taken (empowerment by senior manager/board of directors).

To assist the validator, some examples of validation testing techniques are made available for each criteria within the validator's corner.

The validator's corner is neither an exhaustive list nor a checklist of mandatory elements since there might be other relevant ones.

When conducting the validation, the specific context of the EO (size, role in supply chain, method of operation, etc.) and additional national requirements should also be taken into account.

4.3.2.1 Demonstrated Compliance with Customs requirements and other related laws and regulations

The applicant should not have committed, over a period determined by the national AEO programme, an infringement/offence as defined in national/regional legislation, which would preclude designation as an AEO. This requires the absence of any serious infringement or, where applicable, repeated infringements of legislation related to Customs requirements.

If the applicant has been established for less than the period determined by the national AEO programme, the Customs authorities shall assess compliance with that criterion on the basis of the records and information that are available to it.

The criteria are to be fulfilled by the applicant, or the person in charge of the applicant or exercising control over its management, and the employee in charge of the applicant's Customs matters, also depending on whether the applicant is a natural person or not.

The definition of Customs legislation follows from the national legislation.

The record of compliance with Customs legislation 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.

Infringements of minor importance are those acts that, even if there was an actual infringement of any aspect of the Customs legislation, 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 the event of infringements which could initially be 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. If so, the Customs authorities should analyze 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, meaning that it will not happen again in the future. If, on the other hand, the infringement happens again in different periods of time, this could be an indication of inadequate internal management of the company as far as the adoption of measures to prevent the repetition of such infringements is concerned.

When assessing serious infringements, Customs should take into account the following points:

- ✓ whether there has been deliberate intent or fraud by the applicant;
- ✓ the nature of the infringement;
- ✓ obvious negligence, taking into account the complexity of the Customs legislation, the care taken by the business and its experience and any serious risk indicator with regard to security or safety, and/or Customs.

Serious infringements could also be those that, even where the applicant has not aimed to commit a fraud, are so important as to be considered a serious risk indicator with regard to security and safety, and/or Customs, and where applicable taxation rules and criminal activity relating to the economic activity. Examples of serious infringements are:

Customs legislation and legislation applied by Customs

- ✓ smuggling;
- ✓ fraud, for example deliberate misclassification, undervaluation and overvaluation, or false declaration of origin to avoid payment of Customs duties;
- ✓ infringements related to Intellectual Property Rights (IPR);
- ✓ infringements relating to prohibitions and restrictions;
- ✓ counterfeiting;
- ✓ any other offence related to Customs requirements.

Taxation rules

- ✓ tax fraud
- ✓ tax evasion

Serious criminal offences relating to the economic activity of the applicant

Examples of such serious criminal offences would include:

- ✓ bankruptcy (insolvency) fraud
- ✓ any infringement of health or environmental legislation;
- ✓ participation in a criminal organization;
- ✓ bribery and corruption;
- ✓ cybercrime;
- ✓ money laundering; et,
- ✓ direct or indirect involvement in terrorist activities.

Validators' Corner – Validation testing techniques for the compliance criterion

- ✓ To identify whether the applicant has committed any infringements or offences, over a period determined by the national AEO programme.
- ✓ To consider and assess the difference between any serious, repeated or minor infringements.
- ✓ To determine whether the applicant has committed any serious criminal offences related to his economic activity.

4.3.2.2. Satisfactory system for management of commercial records

The applicant should maintain an accounting system which is consistent with the generally accepted accounting principles applied in the country where the accounts are held, allows validation-based customs control and maintains a historical record of data that enables the user to trace a piece of data from the moment it enters the data system to the time it leaves .

The 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.

The applicant allows the customs authority physical access and electronic access (for those kept electronically) to its accounting systems and, where applicable, to its commercial and transport records. The applicant has a logistical system which identifies location of the goods.

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.

Validators' Corner – Validation testing techniques for assessing the commercial records criterion

- ✓ To have satisfactory procedures in place for the archiving of its records and information and for protection against the loss of information
- ✓ To have physical access to the accounting systems and, where applicable to its commercial and transport records, of the applicant.
- ✓ To carry out cross check between the actual operations, the records kept for customs and the accounting system (whether it is integrated or not)
- ✓ To make transaction tests and ensure there is an audit trail (cross – referring selected bookkeeping entries to their source in order to confirm their accuracy) in the records.

4.3.2.3 Financial viability

Financial viability means good financial standing which is sufficient to fulfill the commitments of the applicant, with due regard to the characteristics of the type of business activity concerned.
Any indication that the applicant is unable or may in the immediate future be unable to meet its financial obligations is to be carefully considered and evaluated.

Validators' Corner – Validation testing techniques for financial viability

- ✓ To determine if the applicant is subject to bankruptcy proceedings.
- ✓ To determine if the applicant has fulfilled (during a certain period) their 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.
- ✓ To determine if the applicant demonstrates on the basis of the records and information available for dedicated period preceding the submission of the

application that they have sufficient financial standing to meet their obligations and fulfil their commitments having regard to the type and volume of the business activity, including having no negative net assets, unless where they can be covered

4.3.2.4 Consultation, Co-operation and Communication

Customs- Business partnership requires the establishment of contact points for both parties. It also requires a mechanism to engage both parties in an open and continuing mutual exchange of information, except information that cannot be released due to law and/or enforcement sensitivities.

As far as the EO is concerned, there is an obligation, through the POC, to timely notify the appropriate Customs contact point of any unusual or suspicious cargo documentation or abnormal requests for information on shipments discovered by employees which is of interest to Customs administrations (cargo bookings, cargo tracking, employee information, etc.) or any other relevant authorities.

Validators' Corner – Validation testing techniques for the consultation, co-operation and communication process

- ✓ To verify if a POC has been formally designated by the EO to contact Customs for all matters identified as being of compliance and enforcement interest to Customs;
- ✓ To assess if the POC is fully knowledgeable about the trade entity's practices and procedures and about the AEO program requirements;
- ✓ To ensure that the POC is empowered to provide direct or indirect access to all information in a timely and accurate manner to the validation team throughout the validation process;
- ✓ To ensure that the POC provides the appropriate access to all relevant places and personnel necessary to conduct the respective validation;
- ✓ To request written procedures/ evidence that the EO has implemented measures in order to notify Customs administration of any AEO compliance issues, including unusual or suspicious cargo documentation or abnormal requests for information on shipments discovered by employees.

4.3.2.5 Education, training and threat Awareness (see also Crisis management and Incident Recovery)

The applicant should have a security plan and a security awareness programme in place which is:

- ✓ dealing with crisis, ensure business continuity and reactivate the entire security system;
- ✓ ensuring that incidents are properly investigated and analyzed to identify rooms for improvement;
- ✓ devising procedures to timely report an incident or a risk situation to the Customs authority ensuring that staff are well informed of the details of the security plan, and will take timely and appropriate remedial measures to respond to security threat scenarios, such as intrusion or unlawful control of an asset within the supply chain, smuggling, breach of information security or cargo integrity, etc.;
- ✓ educate personnel and if appropriate business partners with regard to the risks in the international supply chain and to conducting proper training for staff to acquaint them with the contingency measures.

Validators' Corner – Validation Testing Techniques for Training and Threat Awareness

- ✓ To verify that the personnel or service responsible for security and incident recovery has been appointed,
- ✓ To request written procedures/evidence of implementation that confirms that the EO has established and maintains a security training and threat awareness program,
- ✓ To request a listing of the various security training provided to employees as part of the company's security training programme,
- ✓ To request written procedures and evidence of implementation for their training programme to make employees aware of the procedures the company has in place to address a situation and how to report it,
- ✓ To evaluate the capability to react in a crisis situation (presence, knowledge, capacity),
- ✓ To test if the security awareness and knowledge are disseminated in the company in order to assess the effectiveness of the training programme, and,

4.3.2.6 Information exchange, access and confidentiality: Information Technology (IT) Security (See also satisfactory system of commercial records requirements)

The applicant has satisfactory procedures in place for the archiving of its records and information and for protection against the loss of information and has appropriate security measures in place to protect the applicant's computer system from unauthorised intrusion and to secure the applicant's documentation.

Validators' Corner – Validation testing techniques for IT security

- ✓ To request policies, written procedures /evidence of implementation that confirms that the economic operator has IT security systems in place,
- ✓ To establish who is responsible for managing IT and IT security
- ✓ Verify if the IT systems are accessed by individually assigned accounts (e.g. User Name),
- ✓ To verify segregation of duties: there should be different user profiles connected to the different tasks of the users. Access to master data should be limited,
- ✓ To verify what security features are incorporated into the IT systems (firewall, spyware, encryption, monitoring software etc.),
- ✓ To inquire if the IT systems require a periodic change of password,
- ✓ To request written procedures/ evidence of implementation that confirms that the economic operator has employee training that covers IT security policies, procedures and standards,
- ✓ To-inquire if the EO has monitoring systems in place to identify the abuse of IT including improper access, tampering or the altering of business data.
- ✓ To inquire if the EO takes appropriate actions against employees that abuse/ violate the IT systems,
- ✓ To establish that the EO's IT server room is secured and verify that only authorized employees/ IT personnel have access to it.

4.3.2.7 Cargo and conveyance security:

Security measures should be in place to ensure the integrity of cargo and to prevent irregular practices relevant to the flow of goods (transportation, handling, and storage of cargo) in the international supply chain.

These measures, where appropriate to the business concerned, should 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); and
- loading of goods (including checking quality and quantity and sealing/marking.

How to secure the cargo is secured can vary depending on the type of cargo and means of transport (container, bulk, etc.).

Validators' Corner – Validation Testing Techniques for Cargo and Conveyance Security

- ✓ To request written procedures/evidence of implementation that confirms that the EO has measures in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain,
- ✓ To verify the necessary information related to merchandise/cargo, and ensure it is legible, complete, accurate, and protected against unauthorised exchange, loss or introduction of erroneous information,
- ✓ To verify procedures in place to ensure the data on the transport documents match the actual cargo,
- ✓ To confirm that the EO verifies the physical integrity of the container structure, to include the reliability of the locking mechanisms of the doors, (e.g. 7-point container inspection),
- ✓ To ensure that container inspections are documented and may request a container inspection checklist to verify the information that is being captured,
- ✓ To request to witness a live container inspection process, if possible,
- ✓ To visually verify the secure storage of high security seals that are being used by the EO and confirm how high security seals are logged, purchased and inventoried,
- ✓ To verify the EO is using the adequate high security seals such as ISO 17712

and/or any other customs approved securing mechanism or procedure,

- ✓ To verify that only authorized employees have access to high security seals and are trained,
- ✓ To request, if possible, that the validation team witness how an employee affixes a high security seal,
- ✓ To check how employees, who receive cargo, verify seal information against the respective transport documents, including seal integrity, and,
- ✓ Verify how goods are protected against unauthorized access to storage facilities.

4.3.2.8. Physical Access and Premises Security (appropriate access controls):

Security measures should be in place to prevent unauthorised access to offices, shipping areas, loading docks, cargo areas and other relevant places to secure the access to the premises and to prevent tampering with goods.

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 unauthorized vehicles and goods.

The measures, where appropriate to the business concerned, should include:

- process for access to their premises (buildings, production areas, warehouses etc.) is regulated for staff, visitors, other persons, vehicles and goods;
- procedures that are to be followed if an unauthorised person/vehicle is discovered on company premises (grounds or buildings);
- a site plan for each location of the company that is involved in customs related activities (e.g. layout plan, draft) from which the perimeter, access routes and the location of the buildings can be identified.

Validators' Corner – Validation Testing Techniques for Physical Access/ Premises Security

- ✓ To request and verify written procedures/evidence of implementation that confirms the EO has access controls in place, including the identification and logging of all employees and third parties at all points of entry,
- ✓ To verify whether restricted area's are protected against unauthorized access to staff and/or third parties,
- ✓ To verify how the EO manage the issuance and retrieval of identification badges in order to prevent misuse,

- ✓ To verify if the facility has perimeter barriers which are sufficient and maintained to deter/prevent unauthorized access,
- ✓ To verify if buildings are constructed of materials that resist an unauthorized entry and are maintained by periodic inspection and repair,
- ✓ To verify if appropriate measures are in place to ensure monitoring of vehicles and/or persons at points of entry/exit,
- ✓ To verify, where appropriate, the effectiveness of the video surveillance camera, alarm systems and any other access control system,
- ✓ To verify who is in charge to monitor the security measures and ensures that the prescribed procedures are properly executed.

4.3.2.9. Personnel Security

Security measures should be in place to prevent infiltration of unauthorised staff that could compose a security risk. The main areas that should be always checked include:

- the employment policy of the EO,
- the security screening of prospective employees working in security sensitive positions, such as positions with responsibility for security Customs or recruitment and workplace related to incoming/outgoing goods and storages and
- the policy and procedures when staff leaves or are dismissed

The applicant may also have contractual business relationships with other parties including cleaners, caterers, software providers, external security companies or short-term contractors which 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.

Validators' Corner – Validation Testing Techniques for Personnel Security

- ✓ To request written procedures/ evidence of implementation that confirms that the EO has processes in place to screen prospective employees and contracted persons and to periodically check current employees.
- ✓ To request ,if applicable, written procedures/ evidence of implementation that confirms if a third party company responsible for recruitment has processes in place to screen prospective employees.
- ✓ To verify, to the extent legally possible, if and how background checks of prospective employees are conducted (e.g. criminal, drug testing, financial,

social economic, etc.),

- ✓ To request written procedures/ evidence of implementation that confirms that the economic operator has procedures in place to remove identification, facility and IT system access for employees whose employment has been terminated.

4.3.2.10 Business Partner Security

Security measure should be in place allowing the applicant to clearly identify the 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.

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.

Validators' Corner – Validation Testing Techniques for Business Partner Security

- ✓ To request written procedures/ evidence of implementation confirming that the EO has written and verifiable processes for the selection of business partners and external service providers,
- ✓ To verify if and how (e.g. through questionnaire, security programme certificate, contractual arrangements, security declaration) the EO has taken appropriate measures in order to provide adequate evidence that the business partner can meet an acceptable level of security and safety standards,
- ✓ To request written procedures/ evidence of implementation that confirms that the EO has ensured that business partners develop security processes and procedures consistent with the AEO security criteria to enhance the integrity of the shipment at point of origin,
- ✓ To verify whether the EO inquires any current or prospective business partners have obtained an AEO status and/or part of any other security

based programme,

- ✓ To determine if the subcontractors (for example transporters, hauliers, etc.) are chosen on the basis of their adherence to certain security rules and, where applicable, mandatory international requirements, and a clause preventing further subcontracting,
- ✓ To request if loaded containers are inspected at the subcontractor's premises, the terminal and recipient premises to verify that they have been properly sealed;

4.3.2.11 Crisis management and incident recovery

The applicant has a set of crisis management and a recovery and security plan, to minimize the impact created by a disaster or security incident, and which includes the action points describing the measures to be taken in case of incidents. These plans are to be regularly updated (review programme).

An applicant should have a contingency plan for system disruption in place with satisfactory procedures for the archiving of the company's records and information and for protection against the loss of information. An important aspect of this condition is related to possible destruction or loss of relevant information. Thus, it should be checked whether a security plan exist including action points describing the measures to be taken in case of incidents and whether it is regularly updated Also, any back-up routines when computer systems don't work should be checked.

Validators' Corner – Validation Testing Techniques for crisis management and incident recovery

- ✓ To request written procedures/ evidence of implementation that confirms that the economic operator has established and maintains a security recovery plan that reactivates the security system within a minimum period of time;
- ✓ To verify how incidents are investigated, analysed and how the necessary corrections are implemented ;
- ✓ To verify how the EO reports, on a timely basis, an incident or a risk situation to the Customs authority in the event that a security breach has occurred, or that a potential threat scenario exists, and;
- ✓ To verify how the EO educates personnel and, if appropriate, business partners, with respect to inherent and residual international supply chain risks and corresponding mitigation strategies.

4.2.3.12 Measurement, analyses and improvement

In order to fulfil this requirement, the EO should:

- establish and conduct regular self-assessments of its security management system and supply chain;
- fully document the self-assessment procedure and the responsible parties;
- include in the review assessment results, feedback from the designated parties and recommendations for possible enhancements to be incorporated in a plan for the forthcoming period to ensure continued adequacy of the security management system.

Validators' Corner – Validation Testing Techniques to verify the implementation of measurement, analyses processes and improvement measures

- ✓ To request evidence of implementation that confirms that the economic operator has established and conducted regular in house or external assessments of its internal and supply chain security (the Validator must have access to the report(s)),
- ✓ To request written procedures/ evidence of implementation that demonstrates that the economic operator has continues improvement plans and validation planning in place,
- ✓ To verify the improvements measures recommended have been effectively taken (follow up),
- ✓ To provide, where applicable, recommendations on further improvements based on security assessments reports.

5. REPORTING AND FOLLOW UP

5.1. Reporting

Validators should ensure that the analysis of findings include:

- a clear overview of the EO (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 fulfillment 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 validator;
- the clear recommendation about whether to grant the status or not according to the result of validation process;
- a clear recommendation for the deferment of the decision concerning AEO status, in appropriate cases, until the EO has demonstrated that they have addressed identified deficiencies within the stipulated time;
- where the AEO status is not granted, complete and detailed justifications why the status is not granted
- where AEO status is granted, an overview regarding the AEO risk profile and any recommendations for follow-up

Validators also report findings to Customs management reflecting the overall work already done (risk analysis, validation planning, checks and visits to the premises of the applicant, risk profile of the specific economic operator, etc.) in a summarised and Systemised way and providing clear indications about future actions ;

The final report should include the documentation of supply chain vulnerabilities and best practices that were found throughout the validation process;

5.2. Follow-up of AEOs: Monitoring and Re-assessment

Once the AEO status is granted, one has to differentiate between monitoring and re-assessment. Monitoring is done continuously by customs authorities in the spirit of Customs-Business partnerships to understand, facilitate, and where appropriate, to inspect and regulate the activities of the AEO. This may include visits to his or her premises. It aims at the early detection of any signal of areas for improvements, so that appropriate corrective actions are taken to help the AEO to improve. Where serious non-compliance is detected, monitoring also supports investigation and other regulatory actions that needed to be taken, including re-assessment, suspension, or revocation, as the case may be. Re-assessment implies that serious non-compliance issues have 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. Re-assessment can equally be done periodically based on the validity period of the AEO accreditation to re-confirm the continued compliance to the AEO criteria and suggest potential measure for enhanced compliance.

5.2.1 Monitoring

The ongoing monitoring of the AEO is a joint responsibility of the AEO itself and the Validator or responsible Customs representative. Nevertheless, 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 as appropriate. In fact, AEO security is not a static condition, but rather a fluid situation which is constantly influenced by internal and external changes in world events, corporate culture and government requirements.

Likewise, monitoring is done on a continuous basis by the customs authorities, including through monitoring of the 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 appropriate action in case difficulties or non-compliance are detected. Beside, Customs should maintain an open dialog with the AEO to ensure that the AEO is made aware of newly identified risks/trends or program updates. This can be achieved through scheduled or ad hoc meetings whether in person or telephonically. Any and all updates or enhancements made by the AEO should be effectively communicated and recorded by both the AEO and Customs to guarantee that such improvements are considered when reviewing the AEO profile. Transparency and cooperation between the AEO and Customs is key in enhancing the partnership approach to maximize supply chain security and trade facilitation.

5.2.2 Re-assessment/Re-validation

A reassessment shall be required if there are changes in the legislation specific to, and having an impact on, the conditions and criteria related to AEO status.

A reassessment shall also be required if there are reasonable indications that the conditions or criteria are no longer met. Such indications may arise as a result of monitoring that has been carried out, or information provided by the holder of the AEO authorization, or by other authorities.

6. QUALITY ASSURANCE AND DEVELOPMENT PROGRAMMES

It is recommended that quality assurance and control procedures are established for the review of the performance of validators and managers to ensure a broad uniformity of validating standards.

The aim of quality assurance is to achieve a consistent level of performance by the individual validators as well as consistency of validations audits throughout the Customs Administration, to improve internal processes and enhance the performance of validation procedures and to make sure that identified weaknesses have been evaluated

In order to obtain quality assurance customs should have a comprehensive quality management system in place that could involve a number of procedures and/or methods. The quality management system should focus on:

- The documentation of custom validation work (working papers) and creation of working standards;
- Raising the technological level of processes by the use of up to date technology;
- Raising the professional level and training of customs validators;
- Increasing communication between customs validators, and between the customs validators and the validation managers;
- Minimizing the number of validation errors;
- Improving validating procedures.

Responsibility for quality assurance lies with both the validator and the manager. The Management (head of the validation service, validation managers, validation unit team leaders, etc) has the fundamental role in ensuring that standards of an acceptable quality are being applied to validations. The customs validator can propose improvements to the methodology by taking practical cases into account or provide recommendations for validation procedures.

Customs should also consider an operational policy to cover quality assurance. This could be:

- Define and communicate national policy on validation quality to validators and their managers, e.g. through regular meetings, workshops, newsletters, internet based discussion groups, etc;
- Describe the evaluation tools available to validation managers and define the latter's own managers' role in the quality assurance process;
- Include a process to monitor the quality of validation activity at centralised, operational and policy making level.

Training and development programme

Customs administrations should take the appropriate measures to train validators and keep training them on a continuing basis.

To achieve this goal the administrations should ensure the following:

- The determination of the level of knowledge, skills and competences required for validators;
- The formulation and documentation of detailed training programmes (not only in customs matters but also in IT auditing, accountancy, etc.) to deliver the skills and knowledge required;

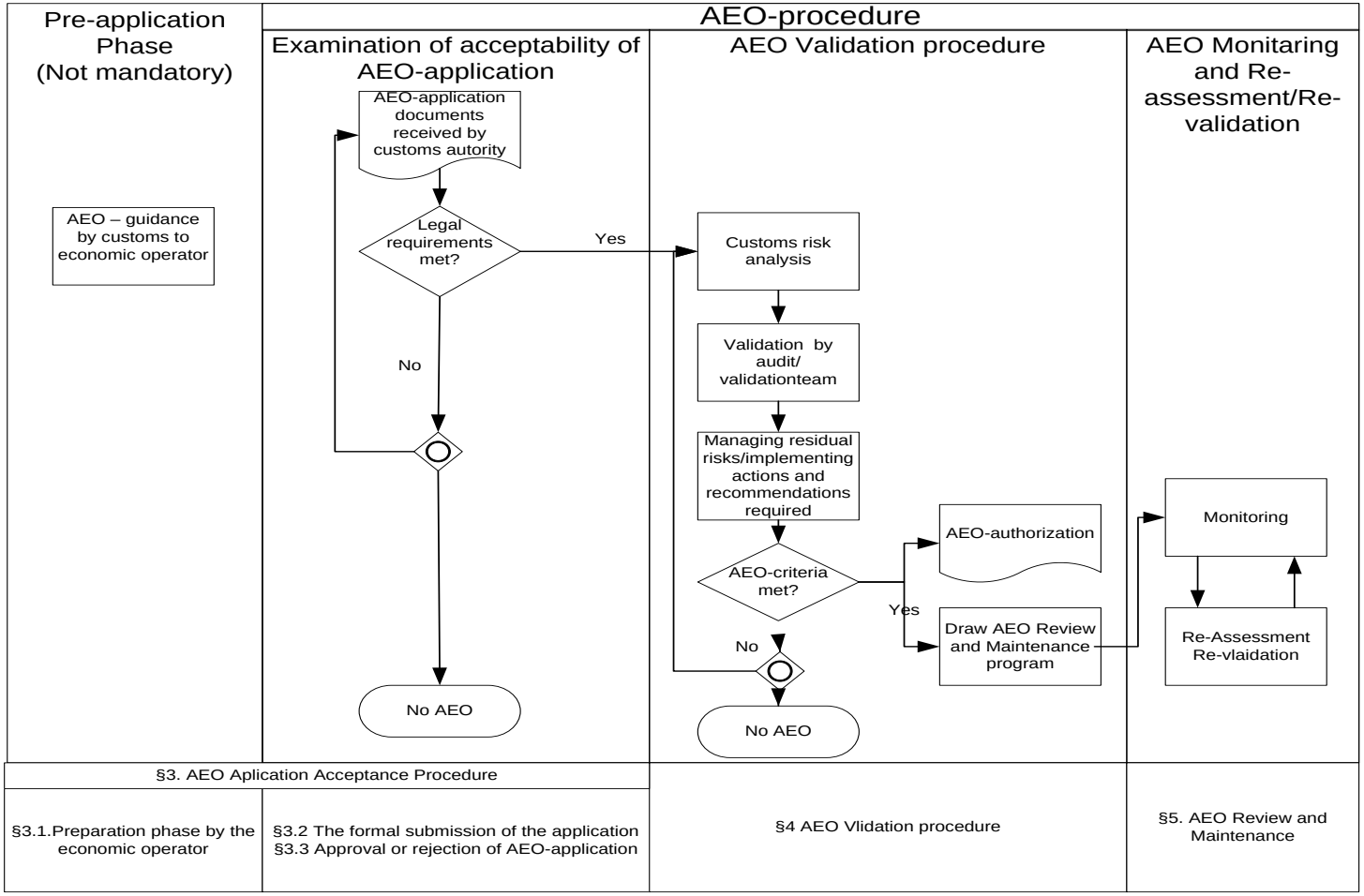
- A sufficient budget for training and IT equipment;
- Team leaders, validation managers, etc. are appropriately trained and have the relevant experience;
- The validator's skills and competences and an assessment of any particular training or support required are reviewed regularly; and
- Development of tools for validators such as checklist, standards templates, functional guidance.

The training programs should cover the following:

- laws and regulations relevant for customs;
- Detailed knowledge of the validation process, techniques, risk assessment, sampling methods, documentation available, etc.
- Accountancy, including international accounting standards and financial analysis;
- An understanding of the business organisation, structures, operations and internal controls of economic operators;
- Knowledge about international trade;
- Updating skills and knowledge (e.g. of new regulations, changes to customs processes and procedures, and enhanced validation techniques established from experience and good practice etc.) through Continuous Professional Development (CPD) ;
- Communication skills, for instance interviewing techniques and debating. Negotiation skills, bad news discussions and conflict controlling;
- Appropriate electronic/IT systems knowledge;
- Practical and personalized training and guidance for newly trained validators when they start working in the daily practice. A mentor should guide the validator for as long as necessary during the validation work. All this is in the context of a good coaching program (student-apprentice-master) to guarantee the necessary connection between theory and practice.

As businesses are different in their size and complexity so will be the skills and knowledge required by the validator who validates those businesses. Training therefore needs to be set at the appropriate level for the type of businesses the validator will be validating.

AEO Flow-chart



ANNEX II

EU's best practices on Auditors and Economic Operators

This annex is not a comprehensive check-list, but an indicative tool to help operators and validators for the management of their AEO programme.

Threats, Risks and Possible solutions

This document provides a list of the **most significant risks related to the AEO autho**risation 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 'Threats, risks and possible solution' document **is addressed both to customs validators and economic operators to facilitate the audit** and examination to ensure compliance with AEO criteria

1. Compliance record

Criterion: An appropriate record of compliance with customs requirements

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	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;	

	related to prohibitions and restrictions, commercial policy, - introduction of goods to the customs territory 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.	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; 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.	

2. The applicants accounting and logistical system

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

2.1. Accounting system

Indicator	Risk description	Possible solutions	References
Computerised environment	The risk that an accounting system is inconsistent with the generally accepted accounting principles applied in the Member	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	ISO 9001:2015, section 6

Integrated accounting system	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. Lack of physical or electronic access to customs and, where appropriate, transport records; Breaching the audit-ability. Inability to readily undertake an audit due to the way in which the applicant's accounting system is structured Complex management	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; implement an enterprise resource planning (ERP); develop training and prepare instructions for the use of the software; allow cross checks of information.	

	system offers possibilities to cover-up illegal transactions. No historical data available.		

2.2. Audit trail

Indicator	Risk description	Possible solutions	References
Audit trail	The absence of an adequate audit trail mitigates against an efficient and effective audit based customs control. Lack of control over the system's security and access.	consultation with the customs authorities prior to the introduction of new customs accounting systems to ensure they are compatible with customs requirements; testing and assuring the existence of the audit trail during the validation phase.	ISO 9001:2015, section 6

Indicator	Risk description	Possible solutions	References
Mix of Customs cleared and non-Customs cleared goods	Lack of logistical system which distinguishes between Customs cleared and non- Customs	internal control procedures data entry integrity checks to verify if the data entries are correct	

	cleared goods. Substitution of Customs cleared and non- Customs cleared goods		

2.3. Internal control system

Indicator	Risk description	Possible solutions	References
Internal control procedures	Inadequate control within the applicant over the business processes. No/weak internal control procedures offer possibilities for fraud, unauthorised or illegal activities. Incorrect and/or incomplete recording of transactions in the accounting system. Incorrect and or incomplete information in customs declarations and other statements to customs.	appointment of a responsible person for quality in charge of procedures and internal controls of the company; make each head of department fully aware of internal controls of their own department; record the dates of internal controls or audits and correct identified weakness through corrective actions; notify the customs authorities if fraud, unauthorised or illegal activities are discovered; make the relevant internal control procedures available to the personnel concerned; 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; appointment of responsible person(s) for managing and updating the customs regulations applicable (inventory of regulations): i.e. update data in the enterprise recourse planning (ERP), clearance	ISO 9001:2015, , sections 5, 6, 7,,and 8

		or accounting, software; Inform and educate staff regarding inaccuracies and how one can prevent them from happening. Having procedures for recording and correcting errors and transactions in place	

2.4. Flow of goods

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.	Information of relevant staff and submission of declaration as scheduled; records of stock movements; regular stock reconciliations; arrangements for investigating stock discrepancies; being able to distinguish in the computer system whether goods are cleared or are still subject to duties and taxes.	ISO 9001:2015, section 6
Incoming flow of goods	Lack of reconciliation between goods ordered, goods received and entries into accounting records.	records of incoming goods; reconciliation between purchase orders and goods received; arrangements for returning/rejecting goods, for accounting and reporting short and over shipments and for identifying and amending incorrect entries in the stock record; formalisation of procedures for import; perform regular inventories; 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.	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.	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.	ISO 9001:2015, sections 6,and 7

2.5. Customs routines

Indicator	Risk description	Possible solutions	References
General	Ineligible use of the routines.	implement formal procedures to manage/follow each customs	ISO 9001:2015,

	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 goods - incorrect tariff code -Incorrect customs value. Lack of routines for informing customs authorities about identified irregularities in compliance with customs requirements.	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; whether or not to receive preferential treatment under a convention or international agreement; 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.	section 6
Representation through third	Lack of control	routines to check third parties work (e. g. on customs declarations) and identifying irregularities or	

parties		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.	
Licences for import and/or export connected to commercial policy measures or to trade in agricultural goods	Ineligible use of goods	standard procedures to record licences; regular internal controls of the licences validity and registration; segregation of duties between registration and internal controls; standards for reporting irregularities; procedures to ensure the use of goods are consistent with the licence.	

2.6 Non-fiscal requirements

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.	

2.7 Procedures as regards back-up, recovery and fall-back and archival options

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-	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	ISO 9001:2015, section 6 ISO 27001:2013 ISO norms for standards in

	up routines. Lack of satisfactory procedures for the archiving of the applicant's records and information. Deliberate destruction or loss of relevant information	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. 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.	the IT security

2.8 Information security – protection of computer systems

Indicator	Risk description	Possible solutions	References
General	Unauthorised access and/or intrusion to the economic operator's computer systems and or programs.	IT security policy, procedures and standards should be in place and available to staff; the presentation of an ISO 27001 certificate demonstrates high standards in IT security; information security policy; information security officer; - information security assessment	ISO 27001:2013

		or identifying issues relating to IT risk; procedures for granting access rights to authorised persons; access rights are to be withdrawn immediately on transfer of duty or termination of employment. -access to data on need to know basis. using encryption software where appropriate; firewalls; anti-virus protection; password protection on all PC Stations and possibly on important programmes If employees leave their workplace the computer should always secured via keyword 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. 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

2.9 Information security – documentation security

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	ISO 28001:2007, section A 4 ISO 27001:2013

		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.	
Security and safety requirements imposed on others	Misuse of the economic operator's information system to endanger the supply chain. Deliberate destruction or loss of relevant information.	requirements to protect data included in contracts; procedures to control and audit the requirements in contracts.	

3. Financial solvency

Criterion: Proven financial solvency

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

Criterion: Appropriate security and safety standards

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.	ISO 28001:2007, section A.4 ISPS Code
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;	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.	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

Indicator	Risk description	Possible solutions	References
Routines for access or entry of vehicles, persons	Unauthorised access or entry of vehicles, persons or	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	ISO 28001:2007, section A.3 ISPS Code

and goods	goods to the premises and/or close to the loading and shipping area.	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.	
Standard operating procedures in case of intrusion	No proper action if intrusion has been discovered.	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; implement remedial measures as a result of incidents related to unauthorised entry.	ISO 28001:2007, section A.3 ISPS Code

4.3. Physical security

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	ISO 28001:2007, section A.3 ISPS Code

		controlled; Irregular patrols of the security staff.	
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	ISO 28001:2007, section A.3
Lighting	Inadequate lighting for external and internal doors, windows, gates, fences	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	

	and parking areas	local power supplies; plans in place to maintain and repair equipment.	
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	

Maintenanc e 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

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; - share planning between the transport department and the goods reception desk.	ISO 28001:2007, section A.3 ISPS Code
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	ISO 28001:2007, section A.3.3 ISPS Code

		discovered; where appropriate supervision by CCTV.	
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.	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.	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.	ISO 28001:2007, section A.3
Standard operating	No proper action if	appropriate procedures laid down on what measures should be	ISO 28001:2007,

procedures in case of intrusion and/or tampering with cargo units	unauthorised access or tampering has been discovered.	taken when an unauthorised access or tampering is discovered.	section A.3

4.5 Logistical processes

Indicator	Risk description	Possible solutions	References
Active means of transport entering/leaving the customs territory	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.	

4.6 Incoming goods

Indicator	Risk description	Possible solutions	References
Routines for checking incoming transport	Introduction, exchange or loss of received goods. Uncontrolled incoming goods which	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	ISO 9001:2015, section 6.2.2 ISO 28001:2007, section A.3

	may pose a security or safety risk.	of the means of transport.	
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.	ISO 28001:2007, section A.3
Supervision 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.	personnel assigned to receive the driver on arrival and supervise the unloading of 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.	ISO 28001:2007, section A.3
Sealing of incoming goods	Lack of control on receipt of goods which may pose a security or	procedures for checking the integrity of seals and the correspondence of the seal number with the number in the documents;	ISO 28001:2007, section A.3 ISO/PAS 17712

	safety risk. Introduction, exchange or loss of received goods	appointment of designated authorised person.	
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.	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.	

4.7 Storage of goods

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.	

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.	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, hazardous goods, high value goods, overseas/domestic goods, air cargo are stored separately.	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.	ISO 28001:2007, section A.3 ISPS Code

4.8 Production of goods

Indicator	Risk description	Possible solutions	References
Assignment of production location Additional security and safety measures for access to goods	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.	ISO 28001:2007, section A.3
Internal control procedures	Lack of procedures to ensure security and safety of manufactured 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	ISO 28001:2007, section A.3

	Tampering with the goods.	process by systems and/or personnel.	
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).	
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

Indicator	Risk description	Possible solutions	References
Routines for checking outgoing transport	Lack of control of delivery of goods which might pose a security or	control the goods loaded (consistency checking / counting / weighing / load order of sales against the information from logistics departments). Check with the logistical system	

	safety risk.	procedures on reception of means of transport are in place; strict access control to the loading area.	
Routines for verifying security measures imposed by others	Breach of agreed security arrangements with the risk of delivery of unsafe or insecure goods; delivery of goods which is not registered in a logistical system and of which you don't have any control.	procedures for ensuring staff are aware of customer's security requirements; management/supervision checks to ensure the security requirements are complied with.	ISO 28001:2007, section A.3
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.	ISO 28001:2007, section A.3
Sealing of outgoing	Sending out goods that	procedures for controlling, applying,	ISO 28001:2007,

goods	are not sealed can lead to introduction, exchange or loss of goods which cannot easily be discovered.	checking and recording seals; appointment of designated authorised person; - use of container seals that are compliant with ISO/PAS 17712.	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.	
Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	procedures to record and investigate irregularities e.g. short shipments, broken ant-tampering devices, customer returns, review procedures and take remedial action.	ISO 28001:2007, section A.3

4.10 Security requirements on business partners

Indicator	Risk description	Possible solutions	Reference
Identification of business partners	Lack of mechanism for clear identification of the business partners.	procedure in place for identifying regular business partners and unknown clients/customers; procedures to select and manage business partners where the transport is carried out by a third	

		party; implement a procedure to select subcontractors based on a list of regular and irregular subcontractors; 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).	
Security requirements imposed on others	Breach of agreed security arrangements with the risk of receiving or delivering unsafe or unsecured goods.	background checks used to select regular business partners e.g. through the use of internet or rating agencies; 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; requirement that contracts will not be further sub-contracted to unknown third parties particularly for the transportation of secure air cargo/air mail; conclusions provided by experts/external auditors, not related to regular business partners, on complying with security requirements; evidence that business partners hold relevant accreditations/certificates to prove they comply with international security standards; procedures for carrying out additional security checks on transactions with unknown or irregular business partners;	ISO 28001:2007, section A.3

		reporting and investigation of any security incidents involving business partners and recording remedial action taken.	

4.11 Personnel security

Indicator	Risk description	Possible solutions	References
Employment policy including for temporary personnel	Infiltration of staff that could pose a security risk.	background checks on prospective employees, e.g. previous employment history and references; additional checks on new or existing employees moving to security sensitive 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	ISO 28001:2007, section A.3

		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.	
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	ISO/28001:2007, section A.3

		relevant areas (loading/unloading etc.). The signs must be visible internally (in the sites) and externally (places dedicated to the drivers, temporaries, various partners).	
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	ISO 28001:2007, section A.3

		year); New staff should be trained intensively due to their lack of knowledge and awareness.	

4.12 External services

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.	ISO 28001:2007, section A.3