World Customs Organization

AEO Implementation and Validation Guidance

2021

wcoomd.org

AEO Implementation and Validation Guidance

2021

World Customs Organization

TABLE OF CONTENTS

Glossary of terms and abbreviations

Authorization	Recognition of AEO status in an AEO programme, based on a structured methodology that includes such processes as a review of an applicant's submitted documentation, physical worksite assets and security processes, to determine compliance with the core international standards of the SAFE Framework. The term is interchangeable with accreditation and certification within this Guidance.
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. (SAFE Framework of Standards Annex I)
Authorized Operator (AO)	An economic operator, provided for under WTO Trade Facilitation Agreement Art. 7.7, who needs to meet criteria, which may include an appropriate record of compliance with Customs and other related regulations, a system of managing records for necessary internal controls, financial solvency and supply chain security, and is therefore entitled to benefit from additional trade facilitation measures.
Business Model	A business model refers to key characteristics about the business, such as roles in the supply chain, size of the business, type of legal entity, types of commodities handled, number of supply chains, and number of partners in the supply chain. Those factors are considered when determining if the company meets AEO criteria.
Business Partner	A business partner is any individual or company that provides a service to fulfil a need within a company's international supply chain. Those roles include all parties, direct or indirect, involved in the purchase, document preparation, facilitation, handling, storage, and/or movement of cargo for or on behalf of AEO importers or exporters. The term is interchangeable with trading partner in this Guidance.
Customs-to-Business Partnership (C-2-B)	One of the key pillars underpinned by the AEO programme under the WCO SAFE Framework, involving close coordination and a robust partnership between Customs and business to create a climate of shared responsibility, ultimately protecting borders and supporting a flourishing trade.
Cybersecurity	The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. (U.S. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency)
Economic Operator (EO)	A person/entity that, in the course of their business, is involved in activities covered by Customs legislation. The term includes, inter alia, importers, exporters, manufacturers, carriers, etc. It is interchangeable with applicant within this Guidance.
Instruments of International Traffic (IIT)	Tools or instruments in use or to be used in the shipment of merchandise in international trade. They include containers, flatbeds, unit load devices (ULDs), lift vans, skids, pallets, etc.

Internal Audit	A measure undertaken by an AEO to review its internal control system, to identify risks and vulnerabilities, and to examine its current status of compliance with authorization criteria. This can be done on a regular basis by a pool of internal staff of the AEO, not necessarily by external professional auditors.
International Commercial Terms (Incoterms)	Incoterms, published by the International Chamber of Commerce (ICC), provide rules and guidance to the trade community, and are often incorporated into contracts for the sale of goods worldwide. They are a series of three-letter commercial trade terms, such as FOB or CIF, and clearly show who pays for what, and when the financial liability is transferred in relation to transportation and delivery of goods.
ISPS Code	Having entered into force as an amendment to the International Convention for the Safety of Life at Sea (SOLAS) in July 2004, the International Ship and Port Facility Security Code (ISPS Code) has since formed the basis for a comprehensive mandatory regime for international shipping. Mandatory Part A outlines detailed maritime and port security requirements which SOLAS contracting governments, port authorities and shipping companies must adhere to in order to be in compliance with the ISPS Code. (International Maritime Organization)
Key Performance Indicators (KPI)	A measurable performance that demonstrates how effectively the Customs has achieved its key objectives and expected results.
Malware	Short for "malicious software", it refers to software that compromises the operation of a system by performing an unauthorized function or process. (U.S. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency)
Monitoring	Monitoring of an AEO is a joint responsibility undertaken independently, and based on their responsibilities, by both the economic operator and Customs. Monitoring is the systematic process whereby Customs and the AEO collect, analyse and use information to track an AEO company's progress and compliance with AEO programme requirements.
Mutual Recognition Arrangement / Agreement (MRA)	Arrangement or agreement to be concluded between and among Customs administrations, whereby they commit to mutually recognize and reciprocally provide trade facilitation benefits to AEOs that have been duly accredited by one Customs administration.
Other Government Agency (OGA)	Agencies of a national government, in addition to the Customs administration, mandated to enforce laws and regulations that deal with international trade and the protection of the supply chain. They include but are not limited to border agencies, transport security agencies and other law enforcement agencies.
Point of Contact (POC)	Economic operator's formally designated representative responsible for the management of the AEO relationship with Customs. AEOs should have more than one AEO POC with Customs.

Private Sector Consultative Group (PSCG)	Established in 2005, the PSCG was formed for the purpose of informing and advising the WCO Secretary General, the Policy Commission and WCO Members on Customs and international trade matters from the perspective of the private sector. The PSCG consists predominantly of businesses/manufacturers and associations.
Quality Assurance	In general terms, it refers to systematic monitoring and evaluation of the various aspects of a project, to ensure that standards of quality are being met. a) In the last stage of the AEO programme implementation lifecycle, the Customs needs to establish the quality assurance procedure to take into consideration lessons learned, experience, and inputs from economic operators and Customs officers in the review process of AEO programme performance (see Chapter I). b) For quality assurance of Customs declarations, an economic operator checks the accuracy and authenticity of Customs declarations made out for a given period (see Chapter II).
Re-Assessment/ Re-Validation	Evaluation process conducted by Customs (and maybe with OGAs) on the AEO company to determine if the AEO company continues to meet its responsibilities as an AEO since it was initially validated/assessed – to include complying with the AEO programme's requirements. As a partnership programme focused on prevention, this process also encourages both parties to discuss security issues and to share best practice that would help secure and expedite the flow of legitimate international trade.
Regulated Agent/Known Consignor (RA/KC)	A regulated agent (RA) is an entity such as a freight forwarder that conducts business with an aircraft operator and provides security controls that are accepted or required by the appropriate authority in respect of air cargo and/or mail. An aircraft operator may also act as a regulated agent. (Section 13.4.2.1 of ICAO Doc. 8973) Known Consignor (KC) refers to a consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of cargo or mail on any aircraft. (Section 13.4.3.1 of ICAO Doc 8973)
Revised Kyoto Convention (RKC)	The International Convention on the Simplification and Harmonization of Customs Procedures (as amended). The RKC aims at facilitating trade by harmonizing and simplifying Customs procedures and practices.
Risk Assessment	Overall process of risk identification, risk analysis, risk evaluation and prioritization. (WCO Risk Management Compendium) The systematic determination of risk management priorities by evaluating and comparing the level of risk against predetermined standards, target risk levels or other criteria. (Guidelines to Chapter 6 of the RKC General Annex)
SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework)	Adopted by the WCO in 2005, the SAFE Framework of Standards to Secure and Facilitate Global Trade sets forth the principles and the standards, and presents them for adoption as a minimal threshold of what should be done by WCO Members in order to secure and facilitate global trade.
Security Standards and Certifications	Certifications under other security-related programmes issued by international trade associations and trade organizations, such as the International Standardization Organization (ISO), the Transported Asset Protection Association (TAPA), and the World BASC Organization (BASC).

Self-Assessment Questionnaire (SAQ)	A document that an economic operator is required to complete in order for Customs to determine if the company is meeting AEO programme requirements. It is part of a process of obtaining or maintaining an operator's AEO status. The SAQ also serves as a useful guide for AEO Validators to deal with the main issues and areas to be addressed during Customs' validation process.
Sensitive Position	Sensitive positions include those in which staff work directly with cargo or its documentation, as well as those in which personnel control access to sensitive areas or equipment. Such positions include, but are not limited to, shipping, receiving and mailroom personnel.
Small and Medium-Sized Enterprises (SME)	Businesses that maintain revenues, assets or a number of employees below a certain threshold. Each Member has its own definition of what constitutes a small and medium-sized enterprise.
Social Engineering	An attack perpetrated through human interaction (social skills), which relies heavily on manipulating people into breaking security standards in order to gain access to IT systems, networks, or physical locations. The attack may involve direct contact with a person or be indirect via email or other methods. (U.S. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency)
Trade Facilitation Agreement (TFA)	An international agreement concluded by members of the World Trade Organization, which entered into force in February 2017. The TFA contains provisions for expediting the movement, release and clearance of goods, including goods in transit. It also sets out measures for effective cooperation between Customs and other appropriate authorities on trade facilitation and Customs compliance issues. It further contains provisions for technical assistance and capacity building in this area. The TFA includes provisions on the Authorized Operator in Article 7.7. (World Trade Organization)
Validation	Procedure whereby the applicants, their supply chain(s), and all relevant processes involved, are subject to a full and transparent review by the Customs to verify that AEO criteria are met. It requires a holistic approach by Validators, from acceptance of the AEO application, to risk analysis, site validation, and findings reporting and follow-up.
Validator	A Customs official or Customs-accredited individual who may be accompanied by other representatives from an OGA who are tasked with conducting the validation process. These government representatives should be equipped with knowledge, skill sets, professional values, ethics and attitudes in order to successfully undertake an effective AEO validation. General competences expected of the Validators are outlined in this Guidance, albeit non-exhaustive.
Vetting	The process of checking a person's or entity's criminal background within the limitations of applicable national law, by: a) The Customs administration to assess the eligibility of AEO applicants (see Chapter I); b) An economic operator, on prospective or current employees in sensitive positions, or the due diligence of their business partners for supply chain evaluations (see Chapter II).
Virtual Re-Validation	A virtual re-validation is a procedure that is conducted virtually or remotely when a physical (on-site) re-validation of an AEO company is not feasible or desirable. Virtual re-validations should only be considered for those AEO companies that have in the past undergone a physical or on-site validation.

Preamble

The World Customs Organization's (WCO) Authorized Economic Operator (AEO) programme has been in existence for more than a decade. It has come to be acknowledged as a key driver in promoting a secure, transparent and predictable trading environment through the voluntary demonstration of compliance and safety and security provisions in trade-related business. International trade is widely recognized as a fundamental driving force for economic prosperity. Given the increasing risks of disruption and terror-related events, the need to ensure that trade takes place within a safe and secure environment is crucial. The modern Customs administration is in a unique position to steward the national safety and security response within the broader context of the global supply chain.

The AEO Implementation and Validation Guidance aims to expand on the existing programmes and practices to assist both Customs administrations and prospective economic operators to secure the international supply chain. This Guidance reflects the commitment both of the WCO and its Members to efficiently facilitate the secure movement of trade by improving the understanding of AEO provisions and standards, and by their collaborative implementation. Ultimately, this will improve the quality and overall uptake of the programme.

The global reach of the AEO programme, combined with the reality that Customs administrations' legislation and strategic policies vary from Member to Member, has led to programme variations. These include significant variations in AEO policies and standard definitions, interpretations and benefits offered, as well as areas of misunderstanding, and areas that are difficult to measure. There is also a general misconception that AEO programmes only benefit large entities and do not provide small and medium-sized enterprises (SMEs) with an incentive to get involved.

The historical variations and success of the AEO programme can be improved through the articulation of tangible benefits and by enhanced levels of cooperation and collaboration amongst the stakeholders. The trading community has a role to play in promoting and facilitating enrolment in the programme and working with national Customs administrations to co-create C-2-B modernization initiatives to support expedited trade facilitation for AEOs.

The AEO Implementation and Validation Guidance aims to collate the best practice, knowledge and lessons learned from the Members, and further considers minimum standards, thus providing a single "outline" in order for Customs and economic operators to align their business operations. These standards are divided into focus areas, ranging from the need for economic operators to demonstrate compliance with Customs requirements, to measuring, analysing and improving the implementation and application of the AEO programme.

The purpose of this Guidance is to assist the AEO process sufficiently by presenting a global, harmonized guide that links to, and builds on, other WCO instruments and tools, particularly the WCO SAFE Framework of Standards and the WCO Revised Kyoto Convention.

According to the AEO Compendium (based on the information provided by Members for 2020), there are currently:

97
operational AEO programmes

20
AEO programmes under development

33
operational Customs compliance programmes

4
Customs compliance programmes due to be launched

87
bilateral and
4
plurilateral/regional Mutual Recognition Agreements (MRAs) concluded

78
MRAs under negotiation

The overview of this AEO Implementation and Validation Guidance is as follows:

CHAPTER I
AEO IMPLEMENTATION AND LESSONS LEARNED

Chapter I outlines the development of an AEO programme. Given that the implementation of an AEO programme is a considerable undertaking, it recommends that Customs administrations follow a typical project lifecycle. This chapter explains the four distinct phases of the lifecycle, using a series of activities and steps that should be considered during the process of AEO development. The order in which the stages or steps are completed may vary, depending on the needs and structure of the Customs administration.

CHAPTER II
AEO TEMPLATE

Chapter II outlines the expected interpretation of the WCO SAFE criteria (A-M) through a globally consistent and harmonized AEO Self-Assessment Questionnaire and accompanying Explanatory Notes. This chapter builds the capacity to implement an AEO programme and encourages WCO Members to adopt it. Furthermore, the standardized approach and the Explanatory Notes will facilitate and clarify what is required under each criterion to implement an AEO programme, potentially encouraging participation in AEO programmes by SMEs.

CHAPTER III
CUSTOMS AEO VALIDATOR GUIDE

Chapter III provides practical guidance to assist Members in carrying out AEO validations in a standardized manner. The chapter also sets out the essential required elements. It further promotes a standard minimum set of competencies of Customs officers (or "AEO Validators") tasked with conducting validations, which would facilitate the efficiency of mutual recognition negotiations.

CHAPTER I.
AEO IMPLEMENTATION AND LESSONS LEARNED

Introduction

The catastrophic events of 11 September 2001 forced Customs administrations around the world to re-assess their roles and develop and implement security programmes. The new international risk landscape also reinforced the need for Customs administrations, in cooperation and partnership with the trade community, to work towards the common goal of securing the international supply chain against terrorism.

Recognizing the need to develop a uniform set of strategies to secure and facilitate the movement of global trade, the WCO engaged with its stakeholders in 2002 to begin the development of Customs guidelines. This work led to the development and eventual adoption in 2005 by the WCO Council of the SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework). The SAFE Framework is intended to act as a deterrent to international terrorism, secure revenue collection, and promote trade facilitation worldwide. In 2007, the WCO's flagship Customs-to-Business Partnership programme – the Authorized Economic Operator (AEO) programme – was introduced.

Implementation of an AEO programme is a significant undertaking and should follow a typical project lifecycle. As outlined below, the project includes a series of activities and steps that should be considered during the process of AEO development. However, depending on the needs and structure of the Customs administration, these stages and/or steps may be completed in a different order.

Before embarking on implementation, it is recommended that **FAQ on linkages between the SAFE Authorized Economic Operator (AEO) programme and Article 7.7 of the WTO Trade Facilitation Agreement (TFA)** be read to ensure there is clarity on the implementation of TFA Article 7.7 in terms of the "Authorized Operator" (AO), and on implementation of the WCO Authorized Economic Operator (AEO).

The SAFE AEO programme and the WTO TFA Article 7.7 – Both the WCO's AEO programme and the World Trade Organization's (WTO) Trade Facilitation Agreement (TFA), Article 7.7, call for trade facilitation benefits for authorized operators who Customs has determine present a low risk of non-compliance with legal requirements. And while the WTO TFA Article 7.7 is a standalone obligation, the AEO is a more comprehensive and all-encompassing programme. Implementation of Article 7.7, however, may nonetheless serve as a stepping-stone towards implementation of a fully-fledge AEO programme (i.e. covering compliance as well as security and safety). Accordingly, implementation of the AEO programme supports fulfilment of the obligations of Article 7.7 of the WTO TFA if at lest three of the seven benefits mentioned therein are included in the AEO program.

Project Lifecycle:
Four Stages for Programme Implementation

STAGE 1

Initiation

- Executive Support
- Analysis and Conceptualization
- Organizational Structure
- Consultation

STAGE 2

Planning, Design and Development of the AEO Programme

- Analysis and Adoption of International Standards
- Develop Programme Requirements
- Resource Allocation
- Legislative Requirements
- Maximize the Use of Technology
- Develop and Deliver Training
- Identify Potential Benefits
- Stakeholder Consultations (Internal, IT, Industry)

STAGE 3

Implementation/ Launch of the AEO Programme

- Conduct a Pilot
- Update/Adjust the Programme
- Secure Funding and Resource Base
- Develop Legislation
- Formally Launch the Programme

STAGE 4

Performance Measurement and Monitoring of the AEO Programme

- Establish Performance Measures
- Establish Quality Assurance and Control Procedures
- Have an Audit/Evaluation Plan in Place
- Develop a Feedback Mechanism for the AEO Programme
- Continued Stakeholder Engagement

STAGE 1 — INITIATION

Executive Support

A successful AEO programme requires senior-level (e.g. Director-General or Executive Committee) support and buy-in to ensure continued support and necessary funding for its development and maintenance.

The decision process must start with the Director-General or Executive Committee. For the programme to succeed, the Director-General must be involved and personally committed from the very start. This commitment is based on public support for the AEO image and on having the necessary resources for its success: an adequate number of Customs personnel who are adequately trained in AEO operations, and the required funding for AEO personnel to conduct their work.

LESSON LEARNED

Given the high turnover rate of Directors-General in some Members, personal commitment by the Director-General might not be enough. The commitment must be formalized via a formal letter to the WCO, and institutionalized as soon as feasible by the establishment of an AEO office within Customs (including by identifying an individual to lead and be responsible for the AEO programme), and by enshrining the establishment of the programme in law.

The Director-General may need to meet with the relevant Minister or higher-level individual to secure the necessary support for the programme. This support at Ministerial level will be critical in terms of other Ministerial offices – particularly those that the AEO programme staff will have to engage with for support. Early engagement of different Ministries that cover border activities will significantly reduce development and implementation problems later. Other important reasons for the Director-General's direct involvement include giving the programme credibility with the trade community, providing tangible support to the team developing the programme, and ensuring that all Customs officers understand the importance of the programme.

Analysis and Conceptualization

Consider conducting an environmental scan of commercial volumes, trade patterns, highest-volume importers/transporters, etc. to better understand the commercial environment, Member-specific risks/threats, as well as governmental priorities. There might be a need to develop a business case for a cost-benefit analysis to outline programme potential, identify resource implications and return on investment, and to outline programme requirements, etc.

Organizational Structure

Create a dedicated section (unit) to deal with the AEO programme, develop a position for an AEO Specialist, and appoint an AEO Coordinator or Director (this must be a high-level position to give the AEO programme its due recognition and visibility).

Once the Director-General has committed to developing an AEO programme, the next step is to form a working group within Customs, tasked with the programme's creation. The Director-General must provide the key strategic objectives for the Customs administration to achieve (for example, mutual recognition with another Member).

The working group will, ideally, include a high-level manager who will serve as the lead, as well as a trade compliance officer, a Customs field officer, a representative from the legal department, and a human resources representative. Other government agencies with authority to inspect arriving or departing international cargo should also participate in this working group.

Consultation

It is important to highlight that private-industry engagement and consultation are essential elements of all stages, from initiation to implementation, and that they should continue as the AEO programme grows and matures. This process will ensure that a healthy and effective partnership is built at the onset, and set the stage for a successful programme.

Consultation on the development of an AEO programme encompasses two distinct critical groups where Customs plays a leadership role. Even

though this is a Customs-to-Business Partnership (C-2-B), as outlined in the second pillar of the SAFE Framework, Customs is the responsible party not only to other Customs administrations, but also as a regulatory agency within its governance structure.

A. **Customs/OGA AEO Working Group**: this group is composed of individuals that represent governmental entities with legal authority at the border. Customs should take the lead in getting all the appropriate parties to the table, introduce the AEO programme to these entities, and determine how each entity can support this important government initiative. Led by Customs, this group is tasked with assessing their current processes and challenges in clearing cargo, and with determining how some of those processes can be expedited, or challenges mitigated, for AEO participants as part of the benefits that will be afforded to the trade community.

   Pillar 3 of the SAFE Framework calls for Customs to engage and cooperate with OGAs regarding the AEO programme. This cooperation and consultation, if carried out early in the AEO implementation process, will help in developing a more comprehensive programme. Several Customs administrations have already included other government agencies as part of their AEO programme (please see the AEO Compendium).

   Raising awareness of the AEO programme and its benefits with other government agencies early in the process, especially by showing agencies how it can benefit the government and the private sector, can help with agency buy-in.

B. **Industry Consultative Group:** develop a consultation working group with members of the private sector to establish trust and commitment (a culture of trust with the private sector needs to be developed or strengthened within Customs and OGAs for the programme to work and benefits to be realized).

   Customs should identify the companies responsible for the majority of the revenue that is collected and invite them to participate in this consultative group. It should also take into account those companies that have considerable participation in trade, in terms of FOB/CIF, or with a complex supply chain. A complex supply chain can provide Customs and OGAs with many vital lessons learned.

   Note: revenue collection is of great importance to many administrations, given that they collect a high percentage of the state budget. Gaining the compliance and membership of these companies will therefore secure a majority of the revenue, thereby mitigating a major concern of some administrations, and allowing them to focus and enlist other companies (including SMEs) through positive reinforcement.

LESSON LEARNED

There may be a need for Customs administrations and the OGAs to overcome a culture of mistrust of the private sector. Partnerships based on shared interests and goals, transparency, and mutual trust and respect, result in a more robust and effective AEO programme.

LESSON LEARNED

If your Customs administration does not have a formal working relationship with the private sector, establish a working relationship from the outset. It is recommended that the WCO's Customs-Business Partnership Guidance be read.

STAGE 2

PLANNING, DESIGN AND DEVELOPMENT OF THE AEO PROGRAMME

In developing the AEO programme, Customs administrations should give serious consideration to the following recommendations.

Analysis and Adoption of International Standards

Customs administrations should, in establishing an AEO programme, make every effort to understand existing standards and, to the extent possible, to adopt those standards as part of their own AEO programme. Such standards include those developed by the WCO and by other Customs administrations with AEO programmes in place. Adoption of those standards is an essential consideration for authorities that hope to sign MRAs with other governments once their programmes have achieved a certain level of maturity. It is important to note, however, that each Customs should feel free to design and implement its programme based on its own risks and needs.

To support SAFE/AEO implementation, the WCO, along with the Private Sector Consultative Group (PSCG) and other stakeholders, has developed several documents. The WCO has compiled a SAFE Package which incorporates all these documents, bringing together this important body of material in one convenient place. For Pillar 2 implementation particularly, some of the key documents that should be studied by Customs personnel in charge of developing and implementing an AEO programme are set out below.

- *AEO Compendium*
- *Model AEO Appeal Procedures*
- *Customs-Business Partnership Guidance*
- *The Authorized Economic Operator and the Small and Medium Enterprise - (FAQs)*
- *Strategy Guide for AEO Mutual Recognition*
- *FAQ on Linkages Between the SAFE Authorized Economic Operator (AEO) Programme and Article 7.7 of the WTO Trade Facilitation Agreement (TFA)*
- *WCO Guidelines on Trader Identification Number (TIN)*

Develop Programme Requirements

Using WCO international AEO standards and guidelines, establish programme requirements for the AEO programme in the following areas: Eligibility, Risk Assessment and Vetting, Supply Chain Security, and Validation and Compliance Requirements. Consider other international partners' programme requirements as a starting point, as well as Member-specific needs.

At this stage, it is important to consider the various business lines the programme will support (e.g. importers/exporters, transporters in each mode, service agents/Customs brokers, freight forwarders, e-commerce).

THE FUTURE AHEAD

The exponential growth of trade in cross-border electronic commerce (e-commerce) has generated enormous opportunities for the global economy, as well as challenges and opportunities to governments. This fast-evolving trading environment requires comprehensive and well-considered solutions from all stakeholders, including Customs administrations – which play a crucial role in the flow of e-commerce shipments. In June 2018, therefore, the WCO adopted the Cross-Border E-Commerce Framework of Standards (E-Commerce FoS), which sets out 15 global standards on cross-border e-commerce, with a view to the provision of pragmatic, fair and innovative solutions. At the same time, these standards take into account the diverse expectations and concerns of Customs administrations and stakeholders.

One of the standards in the WCO's E-Commerce FoS is the expansion of the AEO programme to cross-border e-commerce. That standard encourages Customs administrations to further strengthen their partnerships with the private sector by exploring "… the possibilities of applying AEO programmes and Mutual Recognition Arrangements/Agreements in the context of cross-border E-Commerce". The WCO recommends that Customs administrations implement the FoS in close cooperation with other relevant OGAs and e-commerce stakeholders. All stakeholders of the supply chain should, to the extent practicable and possible, be eligible to participate in the AEO programme – as long as they meet the general conditions and criteria regarding compliance and security. Therefore, the WCO encourages Customs AEO programmes to take these recommendations into account and consider companies engaged in e-commerce as potential members of an ever-evolving AEO programme.

Customs administrations should, to the extent possible, recognize the mandatory security requirements that companies may have already implemented. These include requirements to comply with internationally recognized security norms and standards, or national laws or regulations, when developing security requirements for their AEO operators and when conducting validations of AEO members.

An AEO programme should not duplicate existing security requirements or involve the performance of redundant government validations. Rather, its aim should be to complement the security requirements already in place. Examples of internationally recognized standards include those of ICAO, IMO, UPU, ISO, the World BASC Organization and TAPA.

Resource Allocation

Establish a management structure and team responsible for programme development and delivery. Consider resources for administration, training, delivery, monitoring, reporting, marketing and outreach. Start small but be prepared to expand, based on the volume of potential applicants and work to be undertaken. The establishment of resources dedicated to the development and maintenance of an AEO programme is essential to its ongoing viability.

Legislative Requirements

Consider legislative needs and policies to support the AEO programme. Policy/legislation should include requirements on applying for, and maintaining membership in, the programme. It may also include the requirement that the AEO programme deliver benefits to the private sector. Examples of what to include in policy/legislation are the eligibility criteria to apply, programme-specific requirements, supply chain security, validation timelines, compliance standards, suspension/denial/cancellation criteria, and benefits.

Recognition of a programme, and its compatibility with that of other Members, may be impacted by its legislative authority (or lack thereof).

Maximize the Use of Technology

Consult early with IT departments to maximize use of technology to better manage the AEO programme, to communicate with trade, for electronic applications, data exchange with Members and/or other Customs administrations, potential future MRAs, and for delivery of benefits. It is important to establish a mechanism to identify and recognize AEO members in Customs' processing systems so that benefits can be extended to those members.

Develop and Deliver Training

Officer training is an integral part of ensuring that international standards are met and that officers have the necessary skills to deliver the programme. There is no need to reinvent the wheel. Rather, training should be customized, based on need. The WCO has developed several tools, such as the AEO Validation Module, which contains real-life experiences in implementing and managing a successful programme. The WCO's SAFE Framework and Article 7.7 of the WTO's Trade Facilitation Agreement (TFA) should be part of the training modules.

LESSON LEARNED

It is best to publish the specifics of the AEO programme (i.e. eligibility and security requirements) in a format other than national legislation – which would require an amendment to the law when critical changes or additions to the requirements are necessary. A less formal format would allow the Customs administration to make modifications more swiftly.

Identify Potential Benefits

Consult internally within the Customs organization, with OGAs and with external trade partners, to identify possible benefits for the AEO programme. Consider the WCO's AEO Compendium, which includes benefits provided by other Customs administrations, and ensure benefits are tangible and can be provided to all business lines of the programme.

Consider inclusion of the AEO programme in the Customs administration's business resumption plan or contingency plan. This is an essential consideration as it would help maintain AEO benefits and ensure continuing movement of goods during global health/security crises. This approach would also help strengthen the relationship that AEO programmes should have with the private sector.

For additional lessons learned, the Customs administration should consult the paper "Comments on the Impact of the COVID-19 Crisis: Ideas for the WCO and Its Members from the WCO Private Sector Consultative Group", available on the WCO's website at http://www.wcoomd.org/-/media/wco/public/global/pdf/media/important-notice/pscg-covid_19_en.pdf?db=web.

Stakeholder Consultations (Internal, IT, Industry)

To obtain support for AEO programme enhancements and changes, it is important to engage with internal and external stakeholders during the programme's development stages, and to provide a formal mechanism for government and industry to exchange and discuss programme concepts. Involving private industry from the start, and continuing positive collaboration, will help to ensure the success of the AEO programme.

LESSON LEARNED

While an MRA may be a key objective when establishing an AEO programme, it should be noted that this normally takes place after the programme is fully operational. Potential MRA partners will be looking for a robust, reliable programme that has a certain measure of maturity (number of years the programme has been operational; number of AEO programme members; number of entity types eligible to participate in the AEO programme, etc.).

STAGE 3 — IMPLEMENTATION/LAUNCH OF THE AEO PROGRAMME

Conduct a Pilot

It is highly recommended that a pilot programme be conducted before the AEO programme is formally launched. Consider a few select trusted members to participate in the pilot programme so that processes, system compatibility and benefits delivery are thoroughly tested. The pilot will help Customs determine the extent to which programme requirements are met; whether the objectives for both parties – Customs and trade – are being achieved; and whether processes are efficient, effective and transparent. The pilot results will also help Customs and trade make any necessary adjustments before a formal programme is launched.

Consider the inclusion of large companies in the pilot, as they have leverage over the rest of the supply chain and can, in turn (once the programme is launched), become force multipliers by requiring those business partners to become AEOs (if eligible to participate). But it is also critical to include SMEs in the pilot and so test the extent to which these types of companies can meet the requirements imposed by the AEO programme.

During the course of the pilot, conduct outreach to the trade community, and ensure the Director-General and senior management officials are well informed as to the pilot's progress – particularly if any challenges have been identified, identifying how those challenges may be resolved.

Monitor and evaluate the pilot programme and, based on results, determine when it should be officially launched.

Update/Adjust the Programme

From the lessons learned during the pilot, implement necessary changes to the programme and finalize procedures, processes, etc. Consider how the programme will expand (e.g. as a result of the programme's including additional industry groups or expanding geographically).

Secure Funding and Resource Base

To formally launch the AEO programme, Customs administrations should ensure funding has been secured both for the development stages, and for the necessary ongoing support to increase volumes and expand the programme. This approach should include sufficient funding for the resources required to deliver the programme, as well as for its oversight and policy maintenance.

Develop Legislation

Draft required legislation and finalize programme policies and standard operating procedures. If the Customs administration has already done this, any amendments considered should take into account the lessons from the pilot.

Formally Launch the Programme

Formally launch the programme. The presence of the Director-General, as well as other high-level government officials and international representatives, will give the AEO programme the visibility it needs with the trade community as an important tool for trade to engage in partnership with Customs and its OGAs. AEO pilot participants should have the opportunity to discuss and explain their experience as AEOs, and how being trusted members of the trade community has benefited their operations.

LESSON LEARNED

Do not give into pressure from the trade community to open the programme to too many business entities at the same time or too soon. Keep in mind resources, but also the need to learn and assimilate the lessons to be learned during the first months of programme implementation.

STAGE 4 — PERFORMANCE MEASUREMENT AND MONITORING OF THE AEO PROGRAMME

Establish Performance Measures

Establish key performance indicators (KPIs) to measure the AEO programme's performance. Performance indicators will be critical to demonstrate both internally within the Customs administration, as well as with the private sector, that the programme is achieving the expected results – including the delivery of tangible benefits. This process will also help secure future funding, as this should be a programme that needs to expand, and will further enhance trust with the trade community.

Establish Quality Assurance and Control Procedures

Establish quality assurance and control procedures for the review of the programme's performance. For example, the programme should combine lessons learned from the AEO applicant's experience, with country-specific requirements and new control procedures from AEO programme managers as the work of their administration evolves. The combination of lessons learned and of the new requirements will ensure that overall uniformity of standards is strengthened within the control procedure of the AEO programme.

Have an Audit/Evaluation Plan in Place

Consider conducting periodic programme evaluations and audits to identify areas for improvement, and ensure the programme is performing and meeting its objectives. These evaluations will help ensure the integrity and transparency of the AEO programme.

Develop a Feedback Mechanism for the AEO Programme

The AEO programme must continuously address areas of eligibility, risk assessment and vetting, supply chain security, validation and compliance requirements. International partners' programme requirements, their upgrades and country-specific needs should be considered when the programme is developed and continues to mature. A clear description of all risk areas should be established, as well as follow-up actions for country-specific requirements.

Continued Stakeholder Engagement

As the programme evolves, consider maintaining or conducting regular consultations with the private sector to discuss programme needs, challenges, and future directions. Again, this will help foster the necessary trust and positivity required to ensure a successful and lasting programme partnership.

LESSON LEARNED

Do not be afraid to recognize mistakes – for example, a process might have been designed better or a policy could have been explained sooner. Be prepared to provide a timely solution to the challenges that may arise following implementation.

CHAPTER II.
AEO TEMPLATE

2.1. Introduction

Customs administrations recognize that global consistency of the approval process and enhanced benefits are essential for encouraging broad trade participation and for realizing the mutual benefits of the SAFE Framework and Authorized Economic Operator (AEO) programmes. In support of this objective, a harmonized AEO Application and Self-Assessment Questionnaire has been developed. It can be used by economic operators applying for AEO status in multiple jurisdictions, in electronic or paper form. It covers the main issues and areas to be addressed during Customs' validation of an AEO applicant. Customs administrations are also encouraged to recognize compliance with international security standards and requirements laid down by other intergovernmental organizations.

This document is included in the WCO SAFE Package, which incorporates all tools and guidelines for SAFE implementation. WCO Members building capacity to implement an AEO programme are encouraged to adopt it. A standardized approach will also facilitate the implementation of AEO programmes in developing Members, and potentially facilitate participation in AEO programmes by small and medium-sized enterprises (SMEs).

Customs administrations should recognize the complexity of the international supply chain, and the diverse business models within it. For AEO purposes, "business model" refers to key characteristics about the business that are considered when determining if the company meets the AEO criteria, such as the role of the company in the supply chain, size of the business, type of legal entity, number of supply chains, and number of business partners.

An AEO programme should encourage the implementation of security measures based upon the assessment of risk. The programme should allow for flexibility and the customization of security plans based on the member's business model and the level of risk, as ascertained from the member's own risk assessment. Because flexibility is a cornerstone of the programme, many of the criteria do not contain specific time frames. Instead, language such as "periodic" or "regular basis" is used to allow members to customize their security programmes to fit their circumstances.

For those criteria that require written procedures, it is understood that the latter are being followed or have been implemented by the AEO member (as applicable).

In addition, the harmonized AEO Application and Self-Assessment Questionnaire aims to encourage and facilitate mutual recognition of AEO programmes in order to deliver tangible, transparent and measurable benefits, and will serve as an encouragement to apply for AEO status.

The document should serve as a guideline, giving WCO Members the flexibility to adjust, according to individual domestic requirements consistent with the SAFE Framework. The aim of the Questionnaire is to help economic operators assess whether they meet the criteria to become an AEO and to help them appreciate the requirements associated with obtaining AEO status. At the same time, the Questionnaire will allow Customs administrations to assess those risks that are applicable to the individual applicant. This means that the focus is only on the relevant risks and on particular matters that require attention. Applicants are not required to give an answer to each and every question if the information has already been provided to the Customs administration (or to other clearly indicated relevant government authorities available/accessible to Customs), or if the information is not relevant to the applicant's specific circumstances (in which case the applicant is invited to briefly explain why this is the case).

This document should be considered as a tool for AEO applicants. The Self-Assessment Questionnaire provides detailed explanations, and guides the applicant step by step.

2.2. AEO Criteria Structure Applicable to Self-Assessment Questionnaire

Criteria	ID Number	Sub-Criteria
A. Demonstrated Compliance with Customs Requirements	A.1	Record of Any Infringements/Offences
	A.2	Tax and Customs Duty Payment
	A.3	Quality Assurance of Customs Declarations
B. Satisfactory System for Management of Commercial Records	B.1	Commercial Records Management Framework
	B.2	Commercial Records Management System
	B.3	Internal Control System
C. Financial Viability	C.1	Proven Financial Standing
	C.2	Bankruptcy Proceedings
	C.3	Obligations
D. Consultation, Cooperation and Communication	D.1	Exchange of Information
	D.2	Discrepancy Reports for Goods and Items
	D.3	Emergency Reporting and Contingency Planning
E. Education, Training and Threat Awareness	E.1	Internal Trade Security Training System
	E.2	Education and Training on the Risks Associated with the Flow of Goods and Articles in the International Trade Supply Chain
	E.3	Crisis Management Training and Crisis Management Simulation Exercises
	E.4	Internal Training System on Customs Laws and Regulations
F. Information Exchange, Access and Confidentiality	F.1	Import/Export Activities
	F.2	Data Security

Criteria	ID Number	Sub-Criteria
G. Cargo Security	**G.1**	Safety Management System of Cargo
	G.2	Loading and Receipt of Cargo
	G.3	Export Security
	G.4	Container Safety Management System
	G.5	Container Inspection
	G.6	Container Seals
	G.7	Container Storage
	G.8	Driver Identity Verification
H. Conveyance Security	**H.1**	Security Management System for Conveyance
	H.2	Conveyance Inspection
	H.3	Conveyance Storage
	H.4	Transport Process Control
I. Premises Security	**I.1**	Safety and Security Management System of Premises
	I.2	Exit/Entry
	I.3	Building Structures
	I.4	Lighting
	I.5	Video Surveillance
	I.6	Warehousing Area
	I.7	Locking Devices and Key Custody
	I.8	Access Control Management System
	I.9	Employee Access Control
	I.10	Visitor Access Control
	I.11	Control of Unauthorized Access and Unidentified Persons

Criteria	ID Number	Sub-Criteria
J. Personnel Security	**J.1**	Personnel Security Management System
	J.2	Employee File Management
	J.3	Pre-Employment Review
	J.4	Employee Separation Management
	J.5	Visitor Identification and Registration
	J.6	Identification and Disposition of Unauthorized Access and Unidentified Persons
K. Trading Partner Security	**K.1**	Business Partner Security Control System
	K.2	Comprehensive Assessment
	K.3	Written Documents
	K.4	Regular Checks
L. Crisis Management and Incident Recovery	**L.1**	Contingency Plan
M. Measurement, Analyses and Improvement	**M.1**	Internal Audit/Review Mechanism on Import/Export Activities
	M.2	Monitoring Activities
	M.3	Internal Audit to Assess Continuous Compliance with AEO Criteria
	M.4	Corrective Measures

2.3. Application and Declaration Form

Applicants must submit the following information in order for Customs to initiate the process of determining if the company may be certified as an Authorized Economic Operator (AEO).

The declaration below must also be signed by a company legal representative. This Application and Declaration Form will be part of Customs' AEO record of the company.

Declaration:

I certify that the information I submitted in this application and all the documents that have been or will be submitted to Customs as part of this application for AEO certification are true and correct.

I further understand that any false statements or deliberate omission of critical, pertinent information may result in the denial or revocation of the AEO certificate.

I hereby authorize Customs to begin the process to determine if the company I legally represent may be certified as an AEO – and if so, to conduct the necessary steps for AEO certification.

Signature/Seal of Applicant Title of Person Signing the Document	Date(MM/DD/YYYY)

2.4. General Company Information

AEO APPLICATION	
Company Name	
Company Name (legal entity)	
Countries for which AEO status sought (check all that apply)	
Business Profile	
Business start date (yyyy-mm-dd) / Years in Business / Date of Establishment	
Owner Type (Corporation, Partnership, Sole Proprietor, Wholly Owned Subsidiary, Joint Venture, etc.)	Indicate Type
Principal Businesses (e.g. manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors)	Indicate Business
The nature of the economic activity pursued by the economic operator	
Company website address	
Participation in Customs Programmes	
Detail the ISO country code for all countries in which the economic operator has been admitted to an AEO programme. When the country code is selected, you will be prompted to enter the corresponding authorization number.	Country Code: Authorization Number:
If your company is part of a group, please indicate if any other entities in the group: a) already have an AEO certificate; or b) have applied for AEO status and are currently undergoing an AEO audit by a national Customs administration.	

INFORMATION ON THE LEGAL ENTITY APPLYING FOR AEO STATUS	
Company/Partner Name (legal entity)	
Operating/Doing Business As (if different)	
Business Profile in Country	
Business Number (BN) / Business Code / Importer of Record Number/Country Code/ Economic Operators Registration and Identification (EORI) number	
VAT identification number(s) or N/A	
Business start date (yyyy-mm-dd) / Years in Business / Date of Establishment	
Owner Type (Corporation, Partnership, Sole Proprietor, Wholly Owned Subsidiary, Joint Venture, etc.)	Indicate Type
Business Sectors	
Commercial activities and positions in the international supply chain (e.g. manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors)	

Company Address in Country
Physical address / Full address where the entity was established - Unit number - Street - City - Prov./terr./state - Country - Postal code/zip code - Contact Number - Fax Number
Mailing address (if different) - Unit number - Street - City - Prov./terr./state - Country - Postal code/zip code - Additional delivery info. - Full address where the main activities of the business are carried out - Full address of the office where the Customs documentation is kept
Full address of the office responsible for providing all Customs documentation (If the offices have the same address, indicate “same”)
Full address of the office where the full accounts are kept (If the offices have the same address, indicate “same”)
Multiple Locations - List all locations and their addresses in country covered by this application: - Site Contact Person - Complete Address - Locations where a third party performs outsourced activities for the economic operator

Company Contact Information[1]
Company Contact - First and Last Name - Position Title - Telephone - Fax - E-mail
Alternate Contact - First and Last Name - Position Title - Telephone - Fax - E-mail
Other Certifications
List certifications under other security-related programmes, standards or other national agencies or authorities, if applicable.
Other Company Information
Describe the internal organizational structure of your company (e.g. through an organization chart) and the tasks/responsibilities of each department, and list the names of senior management personnel responsible for areas relevant to this application (e.g. Security, Customs Procedures, Finance, Human Resources).
How many employees do you have in your company?
Please describe any known planned changes to the company's business practices or relationships that will impact the handling of goods or the supply chain currently being used.
Has your company used the same vendors for many years, or does it use seasonal vendors?
In the company vendor base, are relationships formal contractual or informal agreements?
Do you have many foreign source suppliers?
Does your supply chain consist of many commodities or a select few commodities?
Are your logistics service providers established business partners or do they change regularly?

1 In line with their respective legal systems and the requirements on background checks, Customs administrations may include additional questions in self-assessment questionnaires regarding responsible persons in the applicant's company (e.g. date of birth, national identification number, and experience and qualifications regarding Customs matters).

2.5. Self-Assessment Questionnaire

A. DEMONSTRATED COMPLIANCE WITH CUSTOMS REQUIREMENTS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
A.1 **Record of any Infringements/ Offences**	Has your company committed any infringements/offences as defined in national/ regional legislation over a period determined by the national/regional AEO programme?			Although each application to the AEO programme is considered on an individual basis, the applicant requires the absence of any serious infringement or repeated infringements of national/regional legislation, including no record of serious criminal offences relating to the economic activity of the applicant. Customs takes into account the totality of the facts, along with mitigating and aggravating factors (deliberate offence, repeated offences, financial gain, etc.) in its decision to determine if the applicant is qualified to become an AEO. The following are examples of the types of infringements/offences that are considered by Customs under this requirement: Smuggling; fraud (deliberate misclassification, undervaluation, and overvaluation or false declared origin to avoid payment of Customs duties); IPR and trademark violation. The following are examples of the types of criminal offences that are considered by Customs under this requirement: Participation in organized crime/ gangs; direct or indirect involvement in terrorist activities.

A. DEMONSTRATED COMPLIANCE WITH CUSTOMS REQUIREMENTS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Have any designated persons committed any infringements/ offences as defined in national/regional legislation over a period determined by the national/regional AEO programme?			The applicant's designated person also needs to demonstrate compliance with national/regional legislation. The applicant must therefore provide details of any legal actions taken against its designated person (type of offence; date of offence; individuals involved; court judgements; status of the cases, etc.) that will assist Customs in its determination of eligibility. Customs takes into account the totality of the facts, along with mitigating and aggravating factors (deliberate offence, repeated offences, financial gain, etc.) in its decision to determine if the applicant is qualified to become an AEO. The following are examples of the types of infringements/offences that are considered by Customs under this requirement: Smuggling; fraud (deliberate misclassification, undervaluation, and overvaluation or false declared origin to avoid payment of Customs duties); IPR and trademark violations. The following are examples of the types of criminal offences considered by Customs under this requirement: Participation in organized crime/gangs; direct or indirect involvement in terrorist activities.
	Have any applications for Customs authorizations/ certifications been refused, or existing authorizations been suspended or revoked, because of breaches of national/regional legislation over a period determined by the national/regional AEO programme?			Customs must maintain a record of any applications for Customs authorizations/ certifications that have been refused, or a record of existing authorizations that have been suspended or revoked because of breaches of national/regional legislation.

A. DEMONSTRATED COMPLIANCE WITH CUSTOMS REQUIREMENTS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
A.2 **Tax and Customs Duty Payment**	Was there any overdue or unpaid tax or Customs duty payment over a period determined under the national/regional Customs or tax legislation?			Applicants should provide detailed statements on any overdue or unpaid taxes or Customs duties with Customs, and verify the appropriate channel or contact point to address any arrears in Customs duties/tax.
A.3 **Quality Assurance of Customs Declarations**	If you trade in goods that are subject to economic trade licences/restrictions (e.g. textiles, agricultural goods, dual-use goods), please describe briefly your procedures for administering the licences related to the import and/or export of such goods.			Applicants should provide the list of goods they trade in that are subject to economic trade licences/restrictions, and provide the relevant licence/permission or approval from competent authorities. Applicants should be able to describe their procedures for administering the licences/ permissions for the import and/or export of such goods.
	Do you deal in goods subject to anti-dumping or countervailing duties? If so, please provide further information.			Applicants should provide the list of goods they deal with that are subject to anti-dumping or countervailing duties, and should be able to provide further information regarding their actions, as determined by the national/regional legislation.
	Do you perform Customs formalities in your own name and on your own behalf?			Applicants must describe their quality assurance procedures for verifying the accuracy of Customs declarations, including those submitted on their behalf by service providers such as Customs brokers/agents.

A. DEMONSTRATED COMPLIANCE WITH CUSTOMS REQUIREMENTS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Are you being represented by someone regarding Customs formalities (e.g. Customs broker/agent)?			In order to establish their compliance with Customs requirements, applicants should be able to demonstrate the effectiveness of their systems and procedures for meeting such requirements.
	Do you have documented procedures for verifying the accuracy of Customs declarations, including those submitted on your behalf by, for example, Customs brokers?			
	Do you have documented procedures, instructions and guidelines for internal reporting and investigation of breaches connected to Customs-related procedures; and mechanisms for appropriate recording and reporting to Customs?			
	Do you have existing procedures to ensure accurate establishment of Customs values?			
	Do you have quality assurance measures to ensure that the Customs value is correctly established (e.g. checks, plausibility checks, internal working instructions, regular training, and other means)?			

A. DEMONSTRATED COMPLIANCE WITH CUSTOMS REQUIREMENTS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Regarding country of origin: (a) Do you have documented processes that are followed to establish the preferential or non-preferential origin of the imported goods? b) Do you have a defined approach for the issuance of proof of preferences and certificates of origin for exportation?			
	Do you have a defined procedure to ensure correct tariff classification of goods?			
	Do you have quality assurance procedures to ensure that the Customs tariff is correctly established (e.g. checks, plausibility checks, internal working instructions, regular training, and other means)?			
	Do you have a formal documentation retention policy that supports the measures relating to the procedures in place on the establishment of Customs value or tariff?			
	Do you regularly monitor the effectiveness of your quality assurance measures relating to the procedures in place on the establishment of Customs value or tariff?			

B. SATISFACTORY SYSTEM FOR MANAGEMENT OF COMMERCIAL RECORDS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
B.1 Commercial Records Management Framework	Does the company have policies, procedures and/or guidelines in place for the management of commercial records?			At the centre of any records management programme are records management policies. It is important for a company to have a well-written, adopted, and implemented set of policies and procedures. Policies and procedures encourage consistency in how one manages records. They specify what information an organization must keep in the form of records, the procedures for managing those records, retention issues, data security, maintenance and secure disposal. In addition, the manual/guidelines may address items such as business processes and workflow, and the role of records management within them. Guidelines and procedures are designed to help the company and its employees meet their record-keeping obligations and to foster good practice. It is recommended that policies comply with relevant legislative and statutory requirements and international standards. In this context, the company should provide Customs with access to necessary records and make available any authorizations, powers of attorney and licences relevant to the importation or exportation of goods, subject to the requirements of national legislation.
	Is your company subject to any other legislative requirements and standards with regard to management of commercial records, such as laws on data protection, the right to access information, or records management (e.g. ISO 15489)?			
	Does the company give Customs full access to necessary records and make available any authorizations, powers of attorney and licences relevant to the importation or exportation of goods, subject to the requirements of national legislation?			
B.2 Commercial Records Management System	Does the company maintain a commercial records management system, including an accounting system which permits Customs to conduct any required audit aimed mainly at the import and export of goods?			It is important that companies have an effective commercial records management system, as well as accounting system in place. As the creation of vast amounts of information increases and regulatory laws evolve, the need for records management becomes more imperative. However, these systems should provide Customs with insights into the flow of goods and money, as well as the tax aspects, related to import and export. Further, it is also critical that the systems permit Customs to conduct necessary audits in order to fulfil required mandates and obligations effectively.

B. SATISFACTORY SYSTEM FOR MANAGEMENT OF COMMERCIAL RECORDS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Does the system maintained by the company have adequate capability to securely capture, store/archive, process, manage, retrieve, protect and report timely, accurate, complete and verifiable import and export records, with clear procedures defined for Customs purposes?			In the past, maintenance of records mainly equated to maintenance of documents and files. Today, records are kept and managed in many forms, but increasingly, there is a rapid shift to digital. It therefore follows that records need to be made and kept in digital environments. However, whether in digital, manual or hybrid form (digital and manual), it is critical for Customs purposes that the system be well equipped and structured to securely capture, store/archive, process, manage, retrieve and protect data/ information. Further, the system needs to ensure quality data/information and provide timely, accurate, complete and verifiable import and export records with clear procedures outlined. In particular, for Customs purposes, the system should take into account the following: • Proper archiving of records for later presenting to Customs, within any limitations provided under national legislation. • Employment of adequate information technology security measures which will protect against access by unauthorized persons. • Proper procedures laid out for back-up, recovery, fall-back, archiving and retrieval of business records.

B. SATISFACTORY SYSTEM FOR MANAGEMENT OF COMMERCIAL RECORDS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Does the system facilitate a full audit trail of Customs activities or of the tax-relevant movement of goods or accounting entries?			An audit trail, as the name implies, is simply a formal examination, inspection and verification of a path taken. In other words, audit trails are the manual or electronic records that chronologically catalogue events/ transactions or procedures, providing proper documentation and history that are used to authenticate security and operational actions, or mitigate challenges. Numerous companies use versions of an audit trail to provide a historical record of progression, based on a sequence of events/ transactions. These records provide proof of compliance and operational integrity. Audit trails can also identify areas of non-compliance by providing information for audit investigations. Thus, with a good audit trail system in place, Customs will be able to track the flow, recording and management of data/information, documents, transactions, and all the activities relating to import and export of goods. Such a system also provides Customs with documentable proof of the history of a transaction, which ensures accountability. An audit trail of the tax-relevant movement of goods gives Customs the opportunity to cross-check if goods can be surreptitiously introduced in international trade supply chains, and it provides a clear indication of the licit purposes of a transaction.

B. SATISFACTORY SYSTEM FOR MANAGEMENT OF COMMERCIAL RECORDS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
B.3 **Internal Control System**	Does the company have internal control systems which the approving Customs administration finds satisfactory?			Internal control has four basic purposes: safeguarding assets, ensuring financial statement reliability, promoting operational efficiency, and encouraging compliance with the management's directives. Good internal controls are essential to ensuring the accomplishment of goals and objectives. They provide reliable financial reporting for management decisions. They ensure compliance with applicable laws and regulations to avoid unnecessary risk and problems. Poor or excessive internal controls reduce productivity, increase the complexity of processing transactions and increase the time required to do so, and add no value to activities. For Customs purposes, effective internal control needs to: • Ensure that information is complete and accurate; • Minimize opportunities for unintentional errors or intentional fraud; • Ensure systematic control of business activities; • Ensure that financial statements are reliable; • Ensure that good internal/external audit measures are in place; • Ensure compliance with the organization's policies and procedures; and • Ensure that the operations are conducted in accordance with the applicable laws and regulations, providing assurance of proper implementation of Customs procedures and legislation.
	Does the internal control system of your company identify, report to responsible management, rectify and process discrepancies, and ensure proper implementation of Customs procedures and legislation?			

B. SATISFACTORY SYSTEM FOR MANAGEMENT OF COMMERCIAL RECORDS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Have your internal control processes been subject to any internal/external audit, including audit of your Customs routines?			Auditing internal control processes evaluates and ensures the effectiveness of the internal control structure of a company and determines whether the business policies and activities are followed properly. It also ensures that the company meets legal and regulatory requirements, and provides an insight into the effectiveness of its operations. Having comprehensive auditing measures in place thus ensures the auditing of all the company's Customs-related records, information, transactions and activities. This will result in identification of gaps, issues and problems, which should be addressed promptly.
	Does your company have procedures to check computer files (standing data or master files) and does it consider the following risks: a. Incorrect and/or incomplete recording of transactions in the accounting system; b. Use of incorrect or out-of-date information, such as number of articles and tariff codes; c. Inadequate controls of the company processes within the applicant's business, if applicable?			Good internal control processes should make it possible to conduct an effective system audit, even in electronic or digital form (e.g. accounting system), in order to address the internal control shortcomings within a company. For this purpose, a company should have a good procedure with adequate checks and balances, in line with its overall policy framework. That procedure should take into account and encompass all the possible risks. These include the detection, identification and reporting of incorrect, incomplete and/or out-of-date information and transactions which are being maintained and recorded in the system (e.g. tariff classifications, taxes, commodity details) for Customs purposes.

C. FINANCIAL VIABILITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
C.1	**Proven Financial Standing**	Has the company provided financial statements for the previous period, based on national generally accepted accounting principles?			Financial statements based on national generally accepted accounting principles serve as an objective basis on which to determine the financial standing of a company. Where the company is required by national law to have its financial statements audited by an external auditor, these should be provided. If there are opinions or reports attached to the financial statements, these should also be considered. In the case of publicly-held companies, information which is widely available on publicly-held companies may be a useful supplement to the financial statements.
C.2	**Bankruptcy Proceedings**	Is the company currently engaged in, or the subject of, bankruptcy proceedings? Has it ever been?			The applicant should disclose whether the company is or has been the subject of bankruptcy or bankruptcy protection proceedings, and details of the bankruptcy proceedings should be disclosed.
C.3	**Obligations**	Has the company fulfilled its financial obligations regarding payment of Customs duties and all other duties and taxes?			A record of accurate and timely payments to Customs of duties, taxes and fees can serve as evidence of a good compliance record and commitment to meeting Customs obligations over a period of time, reinforcing trust. If a company has met the requirements for financial instruments, such as surety bonds, it is likely to have undergone additional financial screening/underwriting. This should be considered.
		Has the company met requirements for surety bonds or other financial instruments to secure payment of duties and taxes to Customs (in Members which provide for release prior to payment)?			

D. CONSULTATION, COOPERATION AND COMMUNICATION

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
D.1 **Exchange of Information**	Does the business engage in open and continuous information exchange with Customs?			Transparency in communication is key to building trust and encouraging meaningful exchange of information. For example, business can make use of information available on Customs' website, distributing it to its employees and others in the supply chain. Membership in national and international business organizations, especially those that have membership eligibility requirements, provides a channel for regular and ongoing Customs-business dialogue and can promote trust based on the organization's reputation with Customs. Associations may engage in national, regional or international consultative committees, including National Committees on Trade Facilitation under the TFA. This could be at the business or association level, to raise awareness, build trust, manage implementation processes, etc. and could be through formal courses, webinars, or orientation visits to each other's operations.
	Is the business a member or a leader of an industry association which engages in Customs-business dialogue?			
	Is there shared training and professional development between Customs and business?			
D.2 **Discrepancy Reports for Goods and Items**	Are there written documents or electronic data recording differences concerning goods, so that excesses or shortages/deficiencies in goods and articles are reported?			Documented procedures should outline how shortages, overages, and other significant cargo discrepancies or anomalies are investigated and resolved, as appropriate. Likewise, procedures should be in place to promote the efficient and secure flow of information to Customs and law enforcement authorities when security incidents occur or anomalies are detected.

D. CONSULTATION, COOPERATION AND COMMUNICATION

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
D.3 **Emergency Reporting and Contingency Planning**	Are Customs administrations notified in a timely manner if disasters or emergencies occur which involve the goods for Customs purposes?			Companies must have written procedures for reporting to Customs in a timely manner any security-related incidents or anomalies, as well as any incident involving an emergency or disaster. This is to include a description of the facility's escalation process (who is notified first, what and when information is documented, etc.). Notification procedures must include complete and accurate contact information that lists the name(s), phone number(s) and email addresses, if available, of Customs personnel, as well as other law enforcement agencies, as appropriate. Similarly, complete information about contacts for the company must be identified and be accessible. Procedures must be periodically reviewed to ensure contact information is accurate. This is an important part of cooperation, often not considered until something goes wrong. Although there may be separate contingency plans both for business and Customs, these are best developed, or at least reviewed, jointly to ensure clarity and trust as the basis of any action which needs to be taken.
	Does the business have contact information of local Customs at the port of entry and/or exit of goods?			
	Is there joint development and sharing of contingency plans both for Customs and business, including business resumption procedures in the case of systems outages?			

E. EDUCATION, TRAINING AND THREAT AWARENESS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
E.1 Internal Trade Security Training System	Does the business have a documented internal training system for trade security?			One of the key aspects of a company's trade security programme is training. Employees who are aware of security risks and threats, their company's role in the supply chain, and understand why security measures are in place, are more likely to adhere to such measures. Security education ensures that employees receive the training required to identify, prevent and respond to security threats and breaches. Employees must be provided with trade security training on a regular basis, and at least once a year. Newly-hired employees must receive this training as part of their orientation/ job skills training. Contractors must also be provided with security training, based on the job being performed. The training programme must be comprehensive and cover all AEO security requirements.
	Are drivers and other personnel that conduct security inspection of empty conveyances and IIT trained to inspect their conveyances/IIT for security purpose?			Drivers and other personnel that conduct security inspection of empty conveyances and Instruments of International Traffic (IIT) must be trained to inspect their conveyances/ IIT for security purpose. The prevalence of smuggling schemes that involve the modification of conveyances or IIT makes it imperative that drivers conduct inspections of conveyances and IIT to look for serious structural deficiencies.

E. EDUCATION, TRAINING AND THREAT AWARENESS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	As applicable, based on their functions and/or positions, are employees trained on the company's cybersecurity policies and procedures? Does this include the need for employees to protect passwords/ passphrases and computer access?			As applicable, based on their functions and/ or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/ passphrases and computer access. Personnel operating and managing security technology systems must receive operations and maintenance training in their specific areas. Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable. Additional training topics may include protecting access controls, recognizing internal conspiracies, and reporting procedures for suspicious activities and security incidents.
	Are training records maintained so that they may be verified by AEO auditors?			Members must retain evidence of training, such as training logs, sign-in sheets (rosters), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training.
	Have employees operating and managing security technology systems received training on their operation and maintenance? Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable.			Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training programme is usually one that is delivered to applicable personnel in a formal setting, rather than simply through emails or memos.

E. EDUCATION, TRAINING AND THREAT AWARENESS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
E.2 Education and Training on the Risks Associated with the Flow of Goods and Articles in the International Trade Supply Chain	Does the business provide, on a regular basis, education and training on the risks associated with the flow of goods and articles in the international trade supply chain?			It is important for AEO companies to establish and maintain a trade security training and awareness programme in order to recognize and foster awareness of the security vulnerabilities of facilities, conveyances and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. Security training and awareness is not a one-time exercise. Regular security training through various methods is ideal. Routine company-wide updates help ensure security concerns are current and remain "top-of-mind" throughout your organization.
	Do employees understand and are they able to implement processes to ensure the security of goods?			In addition to a record of training completed by employees, companies should have measures in place to verify that the training provided has met all training objectives. Understanding the training and being able to use that training in one's position (for sensitive employees) is of paramount importance. Exams or quizzes, simulation exercises/drills, or regular audits of procedures, etc. are some of the measures that the company may implement to determine the effectiveness of the training.
E.3 Crisis Management Training and Crisis Management Simulation Exercises	Is there periodic training for employees on crisis management, including simulation exercises on crisis response?			A crisis may include the disruption of the movement of trade data due to a cyberattack, a fire, or a carrier driver being hijacked by armed individuals. Based on risk and where the member operates or sources from, contingency plans may include additional security notifications or support, and how to recover what has been destroyed or stolen, with a view to returning to normal operating conditions. Personnel must be trained on how to report security incidents, suspicious activities, and emergencies.

E. EDUCATION, TRAINING AND THREAT AWARENESS

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Are employees aware of what procedures to follow during an emergency response?			Procedures to report security incidents, suspicious activities, and emergencies are extremely important aspects of a security programme. Specialized training modules (based on job duties) may provide more detailed training on reporting procedures, including specifics such as what to report and to whom, how to report an incident, and what to do after the report is completed.
E.4 Internal Training System on Customs Laws and Regulations	Is there documented internal training material on Customs laws and regulations?			A company's compliance with Customs laws and regulations is an essential component of AEO programme eligibility and continued authorization. Specialized training on Customs laws and regulations must be provided to personnel involved in processes within the Customs purview (e.g. import/export documentation, and movement of goods across the border). Training should be specific and relevant to the employee's job responsibilities in complying with Customs laws and regulations (e.g. reporting requirements on imports, or a transport driver's compliance regarding personal effects when crossing the border).
	Is internal training on Customs laws and regulations offered at all levels of the company (management and employees) to make sure knowledge is current?			Training on Customs laws and regulations should be relevant to the employee's role within the company and must be conducted annually so that the employee stays abreast of evolving and emerging schemes.

F. INFORMATION EXCHANGE, ACCESS AND CONFIDENTIALITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
F.1	**Import/Export Activities**	Are there written procedures in place to manage import/export activities?			There should be written procedures for all import/export activities in order to control movements of goods, to ensure that employees are following the same processes, and to prevent errors. This should include a process methodology or flow chart.
		Are import/export management procedures comprehensive, to effectively control the flow of cargo, documentation and information?			
F.2	**Data Security**	Are there documented procedures about the company's information security management system?			Members must have comprehensive written cybersecurity policies and/ or procedures to protect information technology (IT) systems. These policies and procedures must be reviewed annually – or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary. The written IT policy, as a minimum, must address what the company has done in order to: • Defend IT systems against common cybersecurity threats. To this end, a company must install sufficient software/hardware protection against malware (viruses, spyware, worms, Trojans, etc.) and against internal/external intrusion (firewalls) in Members' computer systems. • Ensure that its security software is current and receives regular security updates.
		Has the company adopted information security controls to prevent unauthorized access to, and theft or alteration of, data? Examples of such controls are data authorization management, firewalls and passwords, etc.			

F. INFORMATION EXCHANGE, ACCESS AND CONFIDENTIALITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
				• Prevent attacks via social engineering. • Recover (or replace) IT systems and/or data should a data breach occur or another unforeseen event result in the loss of data and/or equipment. • Regularly test the security of its IT infrastructure if using network systems. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.
				Individuals with access to information technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion that a compromise exists. A system must be in place to identify unauthorized access to IT systems/data or abuse of policies and procedures, including improper access to internal systems or external websites, and tampering or altering of business data by employees or contractors. There should be a policy for controlling access to the IT server room or access list. Only authorized personnel should have access to the server room. Unauthorized persons should ask for permission before accessing the server room, and there should be a record of unauthorized personnel who access the server room.

F. INFORMATION EXCHANGE, ACCESS AND CONFIDENTIALITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Are there disaster recovery back-up plans for data, and other measures to ensure data security?			Procedures should be in place to address the need to back up data. Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format. Data back-ups should take place, as data loss may affect individuals within an organization differently. Daily back-ups are also recommended in case production or shared servers are compromised/lose data. Individual systems may require less frequent back-ups, depending on what type of information is involved. Media used to store back-ups should preferably be stored at a facility off-site. Devices used for backing up data should not be on the same network as the one used for production work. Backing up data to a cloud is acceptable as an "off-site" facility.
	Does the business offer training for employees on information security?			As applicable, based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access. Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training programme is usually one that is delivered to applicable personnel in a formal setting, rather than simply through emails or memos.
	Are penalties or sanctions imposed on the business if there is a violation of the information security policies?			All company personnel that violate the IT cybersecurity policies must be subject to appropriate disciplinary action, which may include termination of employment.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
G.1 **Safety Management System of Cargo**	Is there written documentation to ensure the integrity and security of import/ export goods during transportation, handling and storage?			It is important to have procedures in place to ensure that all information used in the clearing of merchandise/cargo is legible; complete; accurate; protected against the exchange, loss, or introduction of erroneous information; and reported on time. Personnel need to review the information included in import/export documents to identify or recognize suspicious cargo shipments. Relevant personnel need to be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment. If paper documents are used, forms and other import/export-related documentation should be secured to prevent unauthorized use.
G.2 **Loading and Receipt of Cargo**	Is there a process to confirm that the goods loaded conform to the data and/or information on documents regarding such goods, including the weight, labels, number of cases, etc.? Are the suppliers or the goods to be shipped checked using purchase orders or shipping orders?			Arriving cargo should be reconciled against information on the cargo manifest. All shortages, overages, and other significant discrepancies or anomalies need to be investigated and resolved, as appropriate. Information transmitted to Customs should be consistent with the information that appears on the transaction documents provided to the broker. This information includes the supplier and consignee name and address, commodity description, weight, quantity, and unit of measure (boxes, cartons, etc.) of the cargo being cleared.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Are there procedures regarding affixing of signatures and seals, where required?			Sound internal controls dictate that only authorized individuals be allowed to sign company forms and documents, and that procedures governing such authority be in writing and properly disseminated to all affected employees. In addition, controls over seals should be documented, and all concerned personnel should be trained and supervised to ensure compliance with seal security policies and procedures. Documented evidence of the properly installed seal (for example, digital photographs) should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes.
G.3 **Export Security**	Does the business keep records to document how it controls and monitors the safe shipping of exported goods?			Procedures need to be in place to ensure that all information used in the clearing of merchandise/cargo is legible; complete; accurate; protected against the exchange, loss, or introduction of erroneous information; and reported on time. Personnel need to review the information included in import/export documents to identify or recognize suspicious cargo shipments. Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment. If paper documents are used, forms and other import/export-related documentation should be secured to prevent unauthorized use. Departing cargo should be verified against purchase or delivery orders.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Does the business take measures to ensure the secure and safe shipping of goods to be exported (such as shipping monitoring, spot checks, the verification of documents or check of photos, videos, etc.)?			Based on risk, management personnel should conduct random searches of containers and conveyances after the transportation staff have conducted conveyance/IIT inspections. The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random and without warning, so that they do not become predictable. The inspections should be conducted at various locations and times where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to an international border or point of exportation. Documented evidence of the properly installed seal (for example, digital photographs) should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes. The completed 7-point/8-point container inspection sheet (see below) should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.
G.4 **Container Safety Management System**	Are there documented procedures to ensure the integrity and security of the containers?			The prevalence of smuggling schemes that involve the modification of conveyances or IIT makes it imperative that AEO members have written procedures in place outlining how they inspect and document the inspections of conveyances and IIT to ensure the integrity and security of the container/IIT.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
				The inspection process needs to outline written procedures for security inspection purpose. Written procedures must include and describe: How the company ensures that systematic security inspections are being conducted. A 7-point inspection must be conducted on all empty containers and unit load devices (ULDs); and an 8-point inspection must be conducted on all empty refrigerated containers and ULDs: 1. Front wall 2. Left side 3. Right side 4 Floor 5. Ceiling/roof 6. Inside/outside doors, including the reliability of the locking mechanisms of the doors 7. Outside/undercarriage 8. Fan housing (if refrigerated container). The written procedures must also include and describe: How containers are stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure, or (as applicable) allow the seal/doors to be compromised. How conveyances and IIT (such as containers/ULDs) are equipped with external hardware that can reasonably withstand attempts to remove it. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism, must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Is the inspection of all IIT recorded on a checklist?			The inspection of all conveyances and empty IIT must be recorded on a checklist. The following elements should be documented on the checklist: • Container/trailer/IIT number • Date of inspection • Time of inspection • Name of employee conducting the inspection, and • Specific areas of the IIT that were inspected. If the inspections are supervised, the supervisor should also sign the checklist. The completed container inspection sheet should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.
G.5 **Container Inspection**	Prior to loading/ stuffing/packing, do all empty IIT undergo security inspection to ensure their structures have not been modified to conceal contraband. Is a 7-point inspection of all empty containers and unit load devices (ULDs), and an 8-point inspection of all empty refrigerated containers and ULDs, conducted prior to loading/ stuffing?			It is critical that prior to loading/stuffing, all empty IIT undergo a security inspection to ensure their structures have not been modified to conceal contraband. A 7-point inspection of all empty containers and unit load devices (ULDs), and an 8-point inspection of all empty refrigerated containers and ULDs, must be conducted prior to loading/stuffing, to include: 1. Front wall 2. Left side 3. Right side 4. Floor 5. Ceiling/roof 6. Inside/outside doors, including the reliability of the locking mechanisms of the doors 7. Outside/undercarriage 8. Fan housing on refrigerated containers.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
G.6 **Container Seals**	Are written, high-security seal procedures in place that describe how seals are issued and controlled at the facility and during transit? Are procedures in place that provide the steps to take if a seal is found to be altered, tampered with, or has the incorrect seal number, with such procedures including documentation of the event, communication protocols to partners, and investigation of the incident?			Detailed, written high-security seal procedures that describe how seals are issued and controlled at the facility and during transit are critically important. Procedures need to address the steps to take if a seal is altered/tampered with, or if a document has the incorrect seal number. They also need to address communication protocols to partners, and the investigation of the incident. The findings from the investigation should be documented, and any corrective actions must be implemented as quickly as possible. If an AEO member maintains an inventory of seals, company management or a security supervisor must conduct a periodic seal audit that includes taking an inventory of stored seals and reconciliation against seal inventory logs and shipping documents. All audits must be documented. As part of the overall seal audit process, dock supervisors and/ or warehouse managers must periodically verify seal numbers used on conveyances and IIT. These written procedures must be maintained at the local operating level so that they are easily accessible. Procedures must be reviewed at least once a year and updated as necessary.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
				Written seal procedures must include the following elements: **Controlling Access to Seals:** • Management of seals is restricted to authorized personnel. • Secure storage. **Inventory, Distribution and Tracking (Seal Log):** • Recording the receipt of new seals. • Issuance of seals recorded in log. • Track seals via the log. • Only trained, authorized personnel may affix seals. **Controlling Seals in Transit:** • When picking up sealed containers (or after stopping), verify the seal is intact, with no signs of tampering. • Confirm that the seal number matches the one on the shipping documents.
	Are all AEO container shipments that can be sealed, properly secured immediately after loading/stuffing/ packing with a high-security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high-security seals? Qualifying cable and bolt seals are both acceptable.			The sealing of trailers and containers to attain continuous seal integrity continues to be a crucial element of a secure supply chain. Seal security includes having a comprehensive written seal policy that addresses all aspects of seal security, such as using the correct seals, per AEO requirements: a high-security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high-security seals. All seals used must be securely and properly affixed to IIT that are transporting AEO members' cargo from one member to another.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Does the business have documented systems and procedures for attaching and inspecting seals, as well as for reporting seal anomalies or discrepancies?			The following seal verification process must be followed to ensure all high-security seals (bolt/cable) have been affixed properly to IIT, and are operating as designed. The procedure is known as the VVTT process: V – View seal and container locking mechanisms, ensure they are OK; V – Verify seal number against shipment documents for accuracy; T – Tug on seal to make sure it is affixed properly; T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or that any part of the seal becomes loose. **Seals Broken in Transit:** • If a load is examined, record the replacement seal number. • The driver must immediately notify dispatch when a seal is broken, indicate who broke the seal, and provide the new seal number. • The carrier must immediately notify the shipper, broker and importer as to the seal change, and give the replacement seal number. • The shipper must note the replacement seal number in the seal log. **Seal Discrepancies:** • Retain altered or tampered seals to aid in investigations. • Investigate the discrepancy; follow up with corrective measures (if warranted). • As applicable, report compromised seals to Customs and the appropriate foreign government to aid in the investigation.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
G.7 **Container Storage**	Are containers kept in secure areas to prevent unauthorized entry or tampering?			The secure storage of conveyances and IIT (both empty and full) is important to guard against unauthorized access. Conveyances and IIT must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instrument of International Traffic, or (as applicable) allow the seal/doors to be compromised. When cargo is staged overnight or for an extended period of time, measures must be taken to secure the cargo from unauthorized access.
	Are there documented reporting and handling procedures in the case of unauthorized entry into containers or container storage areas?			Procedures must be in place to identify, challenge and address unauthorized/ unidentified persons. Personnel must know the protocol for challenging an unknown/ unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises. Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process. Examples of incidents warranting notification include: • Discovery of tampering with a container/ IIT or high-security seal. • Discovery of a hidden compartment in a conveyance or IIT. • An unaccounted new seal has been applied to an IIT. • Smuggling of contraband, including people; stowaways. • Unauthorized entry into conveyances, locomotives, vessels, or aircrafts. Notification procedures must include accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. Procedures must be periodically reviewed to ensure contact information is accurate.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
G.8 **Driver Identity Verification**	Does the business have information on the conveyance and the identification of the driver in advance of the loading or receipt of goods?			Drivers delivering or receiving cargo need to be positively identified before cargo is received or released. Drivers need to present government-issued photo identification to the facility employee granting access, to verify their identity. If presenting government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the shipment. Prior to arrival, the carrier should notify the facility of the estimated time of arrival for the scheduled pick-up, the name of the driver, and truck number. Where operationally feasible, AEO members should allow deliveries and pick-ups by appointment only. This is designed to help shippers and carriers avoid fictitious pick-ups. Fictitious pick-ups are criminal schemes that result in the theft of cargo by deception. Such deception includes truck drivers using fake IDs and/or fictitious businesses set up for the purpose of cargo theft. When a carrier has regular drivers that pick up goods from a certain facility, it is good practice for the facility to maintain a list of the drivers and their pictures. Therefore, if it is not feasible to let the company know which driver is coming, the company will still be able to verify that the driver is approved to pick up cargo from the facility. A cargo pick-up log must be kept to register drivers and record the details of their conveyances when picking up cargo. When drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pick-up log. Upon departure, drivers must be logged out. The cargo log must be kept secured, and drivers must not be allowed access to it.

G. CARGO SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
				The cargo pick-up log should have the following items recorded: • Driver's name • Date and time of arrival • Employer • Truck number • Trailer number • Time of departure • The seal number affixed to the shipment at the time of departure.
	Does the business have procedures to respond to significant route deviations and late arrivals at the loading dock/area, transfer points, or the final destination?			Both peak and non-peak times must be recorded and incorporated into the tracking process. Waypoints are specific geographical locations defined by sets of coordinates (longitude and latitude) used for navigational purposes, including driving or transit routes. It is recommended that waypoints include the length of time between the yard to the loading point/trailer pick-up, the international border or point of exportation, and the delivery destinations. If a stop is made to collect export documents or to verify seals, these can also be included as waypoints. If GPS technology is employed, geo-fencing must be implemented and is to include alarm notification when a carrier deviates from the assigned route. The parameters for geo-fencing must be set at minimal allowable tolerances for the pre-established transit route.

H. CONVEYANCE SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
H.1 Security Management System for Conveyance	Are there documented procedures to ensure the integrity and security of the conveyance? Is a tracking and monitoring activity log, or equivalent technology (such as GPS), used to track the conveyance while it is en route to an international land border?			It is important for companies to have written procedures to ensure that systematic security inspections are conducted on all conveyances. Prior to loading/stuffing/packing, all conveyances and empty IIT must undergo security inspection to ensure their structures have not been modified to conceal contraband. A tracking and monitoring activity log or equivalent technology, such as a Global Positioning System (GPS), should be used based on risk to monitor shipments or conveyances en route to an international border. If driver logs are used, the driver must record any stops and note that inspections were made of the conveyance, Instrument of International Traffic (IIT) and the seal. The logs should be stored in secured places to guard against unauthorized access. Based on risk, If a GPS tracking system is used, carriers should use a sensor coupling/connector or equivalent technology from the tractor to the trailer to ensure the trailer is also monitored and tracked. Shippers should have access to their carrier's GPS fleet monitoring system so that they may track the movement of their shipments. If driver logs are used, the driver must record any stops and note that inspections were made of the conveyance, Instrument of International Traffic (IIT), and the security seal.

H. CONVEYANCE SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
H.2 Conveyance Inspection	Does the business conduct inspections of conveyances and goods, when required, to prevent the concealment of suspicious or undeclared goods?			It is critically important that conveyances be inspected so that they are not carrying any illegal or undeclared items. Prior to stuffing/packing, all empty IIT need to be inspected, and conveyances must also be inspected if they cross international land borders. However, if an ocean/air-based supply chain is higher-risk, it may warrant more extensive inspection procedures, to include conveyances and/or inspections at marine port terminals or air logistics facilities. Usually, there are higher levels of risk involved in shipments with land border crossings, which is why both the conveyance and IIT undergo additional inspections. For trucks, these systematic inspections must include: **Tractors:** 1. Bumper/tyres/rims 2. Doors, tool compartments and locking mechanisms 3. Battery box 4. Air breather 5. Fuel tanks 6. Interior cab compartments/sleeper 7. Fairing/roof. **Trailers:** 1. Fifth wheel area – check natural compartment/skid plate 2. Exterior – front/sides 3. Rear – bumper/doors 4. Front wall 5. Left side 6. Right side 7. Floor 8. Ceiling/roof 9. Inside/outside doors and locking mechanisms 10. Outside/undercarriage.

H. CONVEYANCE SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
				It is good practice, based on risk, for management personnel to conduct random searches of conveyances after the transportation staff have conducted conveyance/IIT inspections. The searches of the conveyance should be done periodically. Moreover, these searches should be conducted at random and without warning, so that they do not become predictable. The inspections should be conducted at various locations and times where the conveyance is susceptible, such as the carrier yard, or after the truck has been loaded. After a stop, drivers should inspect the conveyance's sealing or locking devices for any signs of tampering prior to resuming the trip. These inspections should be documented. The full outline can also be supported by a review based on the intuition of security personnel, where appropriate.
	Are conveyance inspection records properly documented?			The inspection of all conveyances should be recorded on a checklist. As a minimum, the following elements should be documented on the checklist: • Date of inspection • Time of inspection • Name of employee conducting the inspection • Specific areas of the conveyance inspected. If the inspections are supervised, the supervisor should also sign the checklist.

H. CONVEYANCE SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
	Is there training for employees to understand the purpose of inspection and learn inspection techniques?			Drivers and other personnel that conduct security inspection of empty conveyances and IIT must be trained to inspect their conveyances/IIT for security purposes so that they may understand the threats to the supply chain and what they need to do to mitigate/eliminate those threats. Refresher training must be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures. Inspection training must include the following topics: • Signs of hidden compartments • Concealed contraband in naturally occurring compartments
	Does the company have mechanisms for reporting the concealment of suspicious goods in the conveyance or suspicious alterations to the conveyance?			Procedures to report security incidents or suspicious activity to management and to appropriate authorities are extremely important aspects of a security programme. AEO members must have written procedures for reporting a credible suspicion or an incident, which includes a description of the facility's internal escalation process. Notification procedures need to include accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. AEOs should periodically review these procedures to ensure contact information is accurate. Examples of incidents warranting notification include: • Discovery of tampering with a container/ IIT or high-security seal; • Discovery of a hidden compartment in a conveyance or IIT; • An unaccounted new seal has been applied to an IIT; • Smuggling of contraband, including people; stowaways; • Unauthorized entry into conveyances, locomotives, vessels, or aircraft carriers; • Extortion, payments for protection, threats and/or intimidation.

H. CONVEYANCE SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
H.3 **Conveyance Storage**	Is there a secure area for parking of conveyances to prevent unauthorized entry or other damage?			All cargo handling and storage facilities, including trailer yards and offices, should have physical barriers and/or deterrents that prevent unauthorized access. Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas and conveyances. Locate parking areas outside fenced and/or operational areas – or at least, at substantial distances from cargo handling and storage areas.
	Are there procedures to report unauthorized entry into storage areas or damage to the conveyance?			If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the AEO member must alert (as soon as feasibly possible) any business partners in the supply chain that may be affected, and any law enforcement agencies, as appropriate.
H.4 **Transport Process Control**	Are there administrative control measures concerning the transport units carrying exported goods and articles during the transport process after loading, en route to the point of export?			Companies must have written procedures to protect the integrity of shipping data related to the transport units, such as seal numbers, driver names and their company ID, transport unit's licence plate and/or unit number, unit weight, etc.
	Are there procedures in place to track the conveyance?			Conveyances are tracked to prevent them from being diverted in order to tamper with the load or structure of the conveyance and so allow contraband to be introduced into the shipment. Transportation providers may want to track and monitor their conveyances in real time. Based on risk, If a GPS tracking system is used, carriers should use a sensor coupling/ connector or equivalent technology from the tractor to the trailer to ensure the trailer is also monitored and tracked.

I. PREMISES SECURITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
I.1	**Safety and Security Management System of Premises**	Are there written procedures for managing the safety and security of the business premises?			It is critical for companies to have written procedures to ensure systematic security inspections are conducted throughout the company's premises. A documented periodic inspection should be conducted of all high-risk areas, such as entry/exit gates, building windows, doors, alarm devices, perimeter fencing, exterior lighting, and video surveillance equipment to ensure that structures are adequately protected against unauthorized access or activities, and that any security breaches are detected and reported in a timely manner.
I.2	**Exit/Entry**	Are the entrances and exits to the business premises secured?			Gates where vehicles and/or personnel enter or exit (as well as other points of egress, such as entrances to facilities that are not gated) must be manned or monitored. It is recommended that the number of gates be kept to the minimum necessary for proper access and safety.

I. PREMISES SECURITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
I.3	**Building Structures**	Does the building in which the business operates prevent unauthorized entry?			Preventing unauthorized access to business premises, including offices, warehouse and packing facilities (not agricultural fields), is critical to ensure that company information, conveyances and cargo are not tampered with or stolen. AEO companies need to ensure that these premises have physical barriers and/or deterrents that prevent unauthorized access. Barriers and deterrents (to include fencing, walls, doors, windows, etc.) should be regularly inspected for integrity by designated personnel. If damage is found, repairs should be made as soon as possible. There may also be natural features that are impenetrable, or otherwise impede, access to a facility or building, such as a steep cliff or dense thickets.
		Is the building in which the business operates inspected and repaired regularly to ensure its integrity and safety?			Every building, plant or facility needs to be inspected regularly as part of an overall maintenance programme. The inspection consists of a walk-through survey that allows the individual to visually observe the property, gather information, and note items of interest. Ideally, inspections are scheduled, completed on time, and documented with a report of findings. A competent person should conduct the inspection and the AEO company should take prompt corrective measures to eliminate any hazardous conditions or security gaps. This inspection should include all exterior doors, walls, and widows; exterior lighting; fences, and gates.
I.4	**Lighting**	Is there adequate lighting provided on the premises, including the following areas: exit/entry, cargo and handling of shipment areas, storage areas, fences, parking areas, etc.?			Adequate lighting is an important security feature – both inside and outside the facility – including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas. Automatic timers or light sensors that automatically turn on appropriate security lights are useful additions to lighting apparatus.

I. PREMISES SECURITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
I.5	**Video Surveillance**	Has the company installed security technology, such as video monitoring equipment, to prevent unauthorized entry to the following areas: entrances and exits, loading, unloading and warehousing areas, surroundings of perimeter walls, and parking areas?			Security technology should be utilized to monitor premises and prevent unauthorized access to sensitive areas. Electronic security technology used to secure/monitor sensitive areas and access points includes: burglary alarm systems (perimeter and interior), also known as Intrusion Detection Systems (IDS); access control devices; and video surveillance systems (VSS), including Closed Circuit Television (CCTV) cameras. A CCTV/VSS system could include components such as analog cameras (coax-based), Internet Protocol (IP)-based cameras (network-based), recording devices, and video management software. Secure/sensitive areas which would benefit from video surveillance may include: building entry and reception areas, cargo handling and storage areas, shipping/ receiving areas where import documents are kept, IT servers, rooms where IT servers are stored, yard and storage areas for containers, areas where containers are inspected, and seal storage areas.
I.6	**Warehousing Area**	Are there barriers to prevent the entry of any unauthorized person?			All business structures (offices, warehouses, packing facilities, etc.) must have physical barriers and/or deterrents that prevent unauthorized access. Agricultural fields do not need to comply with these requirements but, based on risk, may want to adopt other security safeguards, such as security patrols.
I.7	**Locking Devices and Key Custody**	Are all internal and external windows and doors of the business premises equipped with locking devices?			Based on risk, internal and external windows and doors should be equipped with locking devices.
		Does the business register the distribution and return of keys?			Members need to have written procedures governing how access devices, such as keys, are granted, changed, and removed. Removal of access devices must take place when the employees separate from the company.

I. PREMISES SECURITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
I.8	**Access Control Management System**	Are there documented processes for the control of vehicles and personnel?			Gates where vehicles and/or personnel enter or exit (as well as other points of egress) must be manned or monitored. It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated.
I.9	**Employee Access Control**	Has the business implemented access controls for employees, such as checking employee ID (containing information such as name, department, photo, etc.)?			Members need to have written procedures governing how identification badges and access devices are granted, changed, and removed. Where applicable, a personnel identification system must be in place for positive identification and access control purposes. Removal of access devices must take place when employees separate from the company. Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes and keys. When employees separate from the company, the use of exit checklists helps ensure that all access devices have been returned and/or deactivated. For smaller companies, where personnel know each other and based on risk, no identification system (such as a company photo identification) is required. Generally, for a company with more than 50 employees, an identification system is required.
		Are there restrictions on access by unauthorized employees to sensitive areas in the building?			Access to sensitive areas must be restricted, based on job description or assigned duties.
		Are employees' vehicles parked in a designated area?			Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas and conveyances. Locate parking areas outside fenced and/or operational areas – or at least, at substantial distances from cargo handling and storage areas.

I. PREMISES SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
I.10 **Visitor Access Control**	Has the business implemented visitor registration processes, including verification of photo ID?			Written processes should be in place and effectively implemented, and are to include the following: Visitors, vendors and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors should be escorted. In addition, all visitors and service providers should be issued with temporary identification. If temporary identification is used, it must be visibly displayed at all times during the visit. The registration log must include the following: • Date of the visit, and visitor's name; • Verification of photo identification (type verified, such as licence or national ID card). Frequent, well-known visitors, such as regular vendors, may forego the photo identification, but must still be logged in and out of the facility; • Time of arrival; • Company point of contact; and • Time of departure.
	Do visitors wear temporary identification badges, and are they escorted by staff?			
	Are visitors' vehicles registered by the business and parked in designated areas?			
I.11 **Control of Unauthorized Access and Unidentified Persons**	Are procedures in place to identify, challenge and address unauthorized/ unidentified persons? Do personnel know the protocol for challenging an unknown/unauthorized person, how to respond to the situation, and are they familiar with the procedure for removing an unauthorized individual from the premises?			Procedures need to be in place to identify, challenge and address unauthorized/ unidentified persons. It is very important for personnel to know the protocol for challenging an unknown/unauthorized person, how to respond to the situation, and to be familiar with the procedure for removing an unauthorized individual from the premises.

J. PERSONNEL SECURITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
J.1	**Personnel Security Management System**	Are there written procedures for screening prospective employees and for performing checks on current employees? Is application information, such as employment history and references, verified prior to employment, to the extent possible and allowed under the law?			Employees are a company's first line of defence against security threats. Application information, such as employment history and references, should be verified prior to employment, to the extent possible and allowed under the law. Employee background screening should include verification of the employee's identity and criminal history, and draw on city, state, provincial, and country databases. Once employed, periodic reinvestigations must be considered, based on cause and/or the sensitivity of the employee's position. Such positions may include those involving access to information, places or systems with security implications. Cause for periodic reinvestigations may include: • Employee re-assignment, retention or promotion; • Job performance; • Conflict of interest; • Unexplained absenteeism; • Unusual changes in an employee's apparent social and economic situation; and • Dishonesty.
J.2	**Employee File Management**	Is there a record of all employees working at the business premises?			The company should have accurate and updated records of its employees, which list, among other things, the names of the employees/contractors; position titles; departments they work for; entry dates and, if applicable, departure date.

J. PERSONNEL SECURITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
J.3	**Pre-Employment Review**	Does the business verify individual identification and employment history before hiring? Is there a policy to review situations where a prospective employee has a criminal record?			Prospective employees should be properly identified with some type of government-issued photo identification (driver's licence, passport, national identification card, etc.). AEO members and their business partners should factor in the results of background checks, as permitted by local statutes, in making hiring decisions. Background checks are not limited to verification of identity and criminal records. In areas of greater risk, they may warrant more in-depth investigations.
J.4	**Employee Separation Management**	Is access to facilities withdrawn and are IDs cancelled for suspended and terminated employees? Does the business prohibit former employees from entering its premises or using its information systems remotely, except when authorized?			Written procedures should outline the company's personnel suspension and termination processes, to include the removal of access devices (keys, badges, etc.) when the employees separate from the company. Companies should consider other items that could be used to compromise access, such as uniforms. The use of exit checklists is recommended to ensure that all access devices have been returned and/or deactivated. Personnel files on employees that have left the company must be kept for a reasonable time.
		Does the business utilize secure IT technology when employees access company systems from outside the office?			Businesses that allow their users to connect remotely to a network should employ secure technologies, such as virtual private networks (VPNs), to allow employees to securely access the company's intranet when located outside the office. Members should also have procedures to secure against remote access by unauthorized users.

J. PERSONNEL SECURITY

ID Number/ Sub-Criteria		Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
J.5	**Visitor Identification and Registration**	Has the company implemented procedures for visitor registration, including visitor name, ID type, visit time, leaving time, etc., and has the business checked the visitor's ID card (including photo) when registering?			Visitors, vendors and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. Some may consider taking photos of visitors upon arrival and later deleting them, in accordance with the privacy laws in their country. The registration log must include the following: • Date of the visit; • Visitor's name; • Verification of photo identification (type verified, such as licence or national ID card). Frequent, well-known visitors, such as regular vendors, may forego the photo identification, but must still be logged in and out of the facility; • Time of arrival; • Company point of contact; and • Time of departure.
		Are all visitors required to wear temporary identification badges?			All visitors and service providers should be issued with temporary identification badges. If temporary identification is mandated by company policy, it should be visibly displayed at all times during the visit.
		Are visitors accompanied by company staff while in the building?			All visitors should be escorted by a company representative throughout the facility, including to such areas as kitchenettes and restrooms.
J.6	**Identification and Disposition of Unauthorized Access and Unidentified Persons**	Are company employees aware of the procedures for identifying unauthorized entry and unidentified persons?			Personnel must be trained on how to identify, challenge and respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises. Personnel must also be trained on how to report all security incidents (such as unauthorized entry and unauthorized persons).

K. TRADING PARTNER SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
K.1 **Business Partner Security Control System**	Are there written procedures outlining criteria for evaluating the supply chain security of business partners?			AEO companies need to have a written, risk-based process for screening new business partners and for monitoring current partners. AEOs need to have procedures in place that outline how they can clearly identify their business partners, and to ensure (through implementation of appropriate contractual arrangements, security declarations or other appropriate measures in accordance with the AEO company's business model) that those business partners also do their due diligence to secure the international supply chain. The following are examples of some of the vetting elements that can help determine if a company is legitimate: • Verifying the company's business address and how long they have been at that address; • Conducting research on the internet on both the company and its principals; • Checking business references; and • Requesting a credit report. Examples of business partners that need to be screened are direct business partners, such as manufacturers, product suppliers, pertinent vendors/service providers, and transportation/logistics providers. Any vendors/service providers that are directly related to the company's supply chain and/or handle sensitive information/equipment are also to be included on the list to be screened; this includes Customs brokers or contracted IT providers.

K. TRADING PARTNER SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
K.2 Comprehensive Assessment	What is the scope of the evaluation made when selecting business partners, and does it include AEO criteria or status?			How in-depth to make the screening of a business partner depends on the level of risk in the supply chain. The business partner screening process can take into account whether a partner is a member of an approved Authorized Economic Operator (AEO) programme with a Mutual Recognition Agreement/Arrangement (MRA) with the member where AEO status was granted. It can also take into account whether the business partner is certified by a recognized security organization that conducts supply chain security audits on its own members, and based on AEO standards. A business partner's certification in an approved AEO programme, or by another recognized security organization, is acceptable proof that the business partner meets programme requirements. Companies must obtain evidence of the certification and continue to monitor these business partners to ensure they maintain their certification. Specific procedures should be in place for identifying regular business partners and unknown companies, including procedures to select subcontractors based on a risk-assessed list of regular and irregular subcontractors. **Subcontractors** In cases where a business partner hires subcontractors to perform any services required under the agreement between companies and the business partner, the companies should be aware of the number of steps of subcontractors that the business partner hires. This should be stated in the agreement. In addition, International Chamber of Commerce (ICC) Incoterms used in buyer/seller transactions can be taken into account when assessing business partners, as additional evidence of business arrangements when assessing the security risks of business trading partners.

K. TRADING PARTNER SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
K.3 **Written Documents**	Does the business encourage its business partners to optimize and improve their trade security processes, and document these in operating procedures or agreements?			Companies that outsource or contract out elements of their supply chain should exercise due diligence (via visits, questionnaires, etc.) to ensure business partners have security measures in place that meet or exceed the AEO requirements. Importers and exporters tend to outsource a large portion of their supply chain activities. Importers (and some exporters) are the parties in these transactions that usually have leverage over their business partners, and can require that security measures be implemented throughout their supply chains, as warranted. To verify adherence to security requirements, importers conduct security assessments of their business partners. The process to determine how much information is to be gathered regarding a business partner's security programme is based on the member's risk assessment and, if there are numerous supply chains, high-risk areas are the priority. Determining if a business partner is compliant with the AEO requirements can be accomplished in several ways. Based on risk, the company may conduct an on-site audit at the facility, hire a contractor/service provider to conduct an on-site audit, or use a security questionnaire. If security questionnaires are used, the level of risk will determine the amount of detail or evidence needing to be collected. More details may be required from companies located in high-risk areas. If a company is sending a security questionnaire to its business partners, consider requiring the following items: • Name and title of the person(s) completing the questionnaire; • Date completed; • Signature of the individual(s) who completed the document * (senior company official, security supervisor, or authorized company representative to attest to the accuracy of the questionnaire);

K. TRADING PARTNER SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
				• Provide enough detail in responses to determine compliance; and • Based on risk, and if allowed by local security protocols, include photographic evidence, copies of policies/procedures, and copies of completed forms, such as IIT inspection checklists and/or guard logs. * Signatures may be electronic. If a signature is difficult to obtain/verify, the respondent may attest to the questionnaire's validity via email, and that the responses and any items of supporting evidence were approved by a supervisor/manager (name and title are required).
K.4 **Regular Checks**	Are there processes to regularly review business partners in the context of building a secure supply chain?			To ensure their business partners continue to comply with all applicable AEO programme requirements, companies should update their security assessments of their business partners on a regular basis, or as circumstances/ risks dictate, and at least annually. Periodically reviewing business partners' security assessments is important to ensure that a strong security programme is still in place and operating properly. If a company never requires updates of its assessment of a business partner's security programme, it will not know if a once viable programme is no longer effective, thus putting the company's supply chain at risk. Deciding on how often to review a partner's security assessment is based on the company's risk assessment process. Higher-risk supply chains would be expected to have more frequent reviews than low-risk ones.

K. TRADING PARTNER SECURITY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
				If a company is evaluating its business partner's security via in-person visits, it may want to consider leveraging other types of required visits. For example, it may consider cross-training personnel that test for quality control to also conduct security verifications. Circumstances that may require the self-assessment to be updated more frequently include an increased threat level from a source country, changes in source location, or new critical business partners (those that actually handle the cargo, provide security to a facility, etc.).

L. CRISIS MANAGEMENT AND INCIDENT RECOVERY

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
L.1 **Contingency Plan**	Has a contingency plan been put in place to respond to disasters and emergencies, and is it updated in a timely manner?			Companies should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption. A crisis or emergency may include the disruption of the movement of trade data due to a cyberattack, a fire, or a carrier driver being hijacked by armed individuals. Based on risk and where the member operates or sources from, contingency plans may include additional security notifications or support; and how to recover what was destroyed or stolen, in order to return to normal operating conditions. Contingency plans need to be updated, based on risks and lessons learned.

M. MEASUREMENT, ANALYSES AND IMPROVEMENT

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
M.1 **Internal Audit/Review Mechanism on Import/Export Activities**	Does the company have internal mechanisms in place to continuously audit/review import/ export activities and to document its records?			The goal of an internal audit/review is to ensure that employees are following the company's procedures. The company decides the scope of the audit/review and how in-depth it should be – based on its role in the supply chain, business model, level of risk, and variations between specific locations/sites. The internal audit/ review activities are usually conducted by company employees.
M.2 **Monitoring Activities**	Does the company conduct regular monitoring activities against AEO criteria?			The internal audit/review activities need to be performed regularly, i.e. once a year. A member may choose to use smaller targeted reviews directed at specific procedures. Specialized areas that are key to supply chain security, such as inspections and seal controls, may undergo reviews specific to those areas. However, it is useful to conduct an overall general review periodically to ensure that all areas of the security programme are working as designed. For members with high-risk supply chains (determined by their risk assessment), simulation or table top exercises may be included in the audit to ensure personnel will know how to react in the event of a real security incident.
	Does the company keep records of monitoring activities?			
M.3 **Internal Audit to Assess Continuous Compliance with AEO Criteria**	Does the company perform regular internal audits to assess continuous compliance with AEO criteria?			The role of internal audit is to provide independent assurance that a company's risk management, governance and internal control processes are operating effectively. A review process of AEO requirements may be included in the context of internal control of the company.

M. MEASUREMENT, ANALYSES AND IMPROVEMENT

ID Number/ Sub-Criteria	Questions	Yes	No	Explanatory Notes – If the answer is Yes, follow the instructions to prepare documents/evidence; if it is not applicable, provide an explanation below.
M.4 **Corrective Measures**	Does the company have internal mechanisms in place to continuously improve import/export activities and address issues identified in audits/reviews?			If weaknesses are identified during business partners' security assessments, they must be addressed as soon as possible, and corrections must be implemented in a timely manner. Companies must confirm via documentary evidence that deficiencies have been mitigated. There will be different timelines for making corrections, based on what is needed for the correction. Installing physical equipment usually takes longer than a procedural change, but the security gap must be addressed upon discovery. For example, If the issue is replacing a damaged fence, the process of purchasing a new fence needs to start immediately (addressing the deficiency), and the installation of the new fence (the corrective action) needs to take place as soon as it is feasible. Based on the level of risk involved and the importance of the weakness found, some issues may require immediate attention. If it is a deficiency that may jeopardize the security of a container, for instance, it should be addressed as soon as possible. Examples of documentary evidence may include copies of contracts for additional security guards, photographs taken of a newly installed security camera or intrusion alarm, or copies of inspection checklists, etc.
	Has the company implemented mechanisms for establishing accountability when the company's activities do not conform to AEO requirements?			
	Have the corrective measures required by Customs been carried out by the legal representative (person in charge) or senior managers in charge of Customs affairs?			

CHAPTER III.
CUSTOMS AEO VALIDATOR GUIDE

3.1. Introduction

The WCO SAFE Framework of Standards to Secure and Facilitate Global Trade (the SAFE Framework) incorporates the AEO concept and serves as a starting point for national AEO programme implementation. The Framework thus underpins the practical application of the standards and information outlined in its Pillar II (Customs-to-Business Partnerships) and in Annex IV.

This chapter provides practical guidance to assist Members in carrying out AEO validations in a standardized manner. It sets out the essential elements required, and promotes a common minimum set of competencies of Customs officers tasked with conducting validations.

The AEO concept is based on a partnership between Customs and the economic operator. That relationship should be based on the principles of transparency, fairness, responsibility, and mutual respect for the other's role.

The AEO programme's goal is to promote supply chain security and trade facilitation at a global level in order to allow certainty and predictability of trade movement across international borders. This is done by applying standards that enable a harmonized and integrated approach to supply chain management for all participants in the international supply chain.

AEO status is only granted to an economic operator that satisfies the criteria outlined in the AEO Self-Assessment Questionnaire of Chapter II. In the light of this, a particular standard for each qualification criterion (A to M) should be established to validate the partnership between Customs and the economic operator.

Consequently, AEO validation and the role played therein by the AEO Validator are paramount for the AEO concept. Since the AEO validation procedure (including re-assessment/re-validation and/or monitoring processes) is risk-based, it aims to verify that the applicant meets and continues to meet the requirements of AEO authorization.

THIS CHAPTER IS DESIGNED TO ASSIST VALIDATORS IN CONDUCTING THE CUSTOMS AEO VALIDATION CONTROLS. THE SPECIFIC AIMS ARE TO:

- Create a set of competencies ensuring that the AEO Validator is sufficiently equipped to conduct an AEO validation;
- Set out essential elements needed to conduct an AEO validation, based on the completed Self-Assessment Questionnaire;
- Provide practical guidance through the sharing of techniques and expertise to assist AEO Validators in carrying out AEO validation in a standardized manner;
- Promote a common approach to the Customs AEO validation process and apply working methods suited to the national, regional and international context;
- Facilitate the efficiency of mutual recognition negotiation and implementation processes, since the validation process is intended to be harmonized, with the same outcomes from all AEO applicants; and
- Provide practical guidance in developing procedures for conducting on-site validations, virtual re-validations, or a hybrid approach to validations.

The AEO validation must be carried out within a timeframe defined by Customs in collaboration with the private sector, and/or by legislation, before the granting of AEO status.

Risk-based validation requires the Validator to:

- Make a judgement about the fulfilment of the conditions for the granting of AEO authorization;
- Identify and evaluate the relevant risks, assess the remaining risks, and propose and take further action where necessary;
- Identify elements in the operator's procedures which need closer Customs monitoring, and advise the applicant on how to improve or strengthen the relevant procedures and controls.

In cases where the AEO Validators have identified gaps, the economic operator must follow up by implementing an action plan to address the "actions required" and/or recommendations issued during the AEO validation process, in order to mitigate any identified risks. To conclude this process, evidence of compliance which satisfies the requirements must be provided.

Once AEO authorization has been granted, monitoring may consist of confirmation based on risk or cause and, where appropriate, random spot checks by Customs. These checks should be performed on an ongoing basis and could result in re-assessment or the need for re-validation, including through monitoring of the day-to-day activities of the AEO and, if needed, visits to the EO's premises. Monitoring is aimed at the early detection of any sign of non-compliance, which would lead to prompt actions to rectify the situation.

Re-assessment can result, inter alia, from structural changes in operations, new legislation, or other reasonable indications that action should be taken to verify whether the economic operator continues to meet the AEO criteria.

To maintain the level of compliance with the obligations resulting from the AEO authorization, the AEO must inform Customs of any circumstances that may impact its AEO authorization.

The AEO must also appoint a person within its management structure to be responsible for communicating with the Customs administration regarding the AEO approval system and the maintenance of standards.

A team of Customs Validators led by a team leader will conduct the AEO validation. The objective is to put an organizational structure in place that enables the team to perform their tasks efficiently and effectively. Validators are responsible for carrying out the AEO validation in the most effective way, applying the appropriate AEO validation procedures and techniques correctly, and ensuring compliance with established criteria. Team leaders 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.

3.2. AEO Validator(s) Profile

3.2.1. Introduction

Annex IV to the SAFE Framework provides that the Customs administration must ensure that personnel designated to conduct the validation procedure are trained and qualified.

The team of Validators should possess all the core values and skills listed below, including those relating to professional values, ethics and attitude.

They should also have the correct and relevant knowledge to verify the AEO requirements. Specialists may be used for more complex issues, such as IT security. The size and complexity of the EO's business activity determines the need for a specialist.

It is highly recommended that officers gain relevant practical experience by accompanying more experienced Validators. In cases of newly developed AEO programmes, Customs administrations may seek assistance from other established AEO programmes and/or WCO experts, as well as from internationally recognized compliance/security validation programmes, such as ISO, BASC and TAPA.

3.2.2. 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 the AEO criteria (A to M), as set out in the Self-Assessment Questionnaire;
- Knowledge of the national AEO programme (legal background; benefits, eligibility requirements; suspension and removal policies, etc.);
- 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 and the history of the AEO concept;
- 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 book-keeping and IT applications for financial accounting and reporting;
- Knowledge of information technology, including IT security;
- Basic knowledge of multiple languages, where needed;
- Knowledge of safety and security programmes of other government or inter-governmental agencies (for example Regulated Agent/Known Consignor, and ISPS Code);
- Knowledge of relevant commercial standards and certifications (for example ISO, BASC and TAPA);
- Knowledge of bilateral or multilateral treaty obligations and local cultures;
- Knowledge of the global supply chain; and
- Knowledge of industry best practice.

Skills requirements:

- Ability to identify and solve problems;
- Ability to undertake appropriate technical research;
- Ability to liaise with Customs, OGAs 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 regard 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 organization; and
- Ability to communicate effectively in writing, including via written reports.

Note: the requirements can be covered by an individual and/or a team.

Professional values, ethics, and attitudes:

The fundamental principles are set out below.

- 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 judgements. Customs Validators must be independent and impartial, and must be seen to be so. Validators should declare any prejudicial factors or conflicts of interest that may impact on their dealings with a particular operator (e.g. the relationship between Validators and operators or shareholders).
- Professional competence and due care: Validators must apply the knowledge, skills and experience needed to conduct a Customs validation. Validators must also be aware of their national Customs administration's specific Code of Conduct and fully comply with its requirements.
- Confidentiality: Customs Validators are required to protect the privacy of individuals and economic operators in official dealings, as per national legislation.
- Professional behaviour: at every step of processing an AEO authorization, Validators must be mindful of the image of Customs and the AEO programme they are representing. For this reason, they must act professionally and remain permanently attentive to the operator's questions and/or concerns, responding in a professional manner.

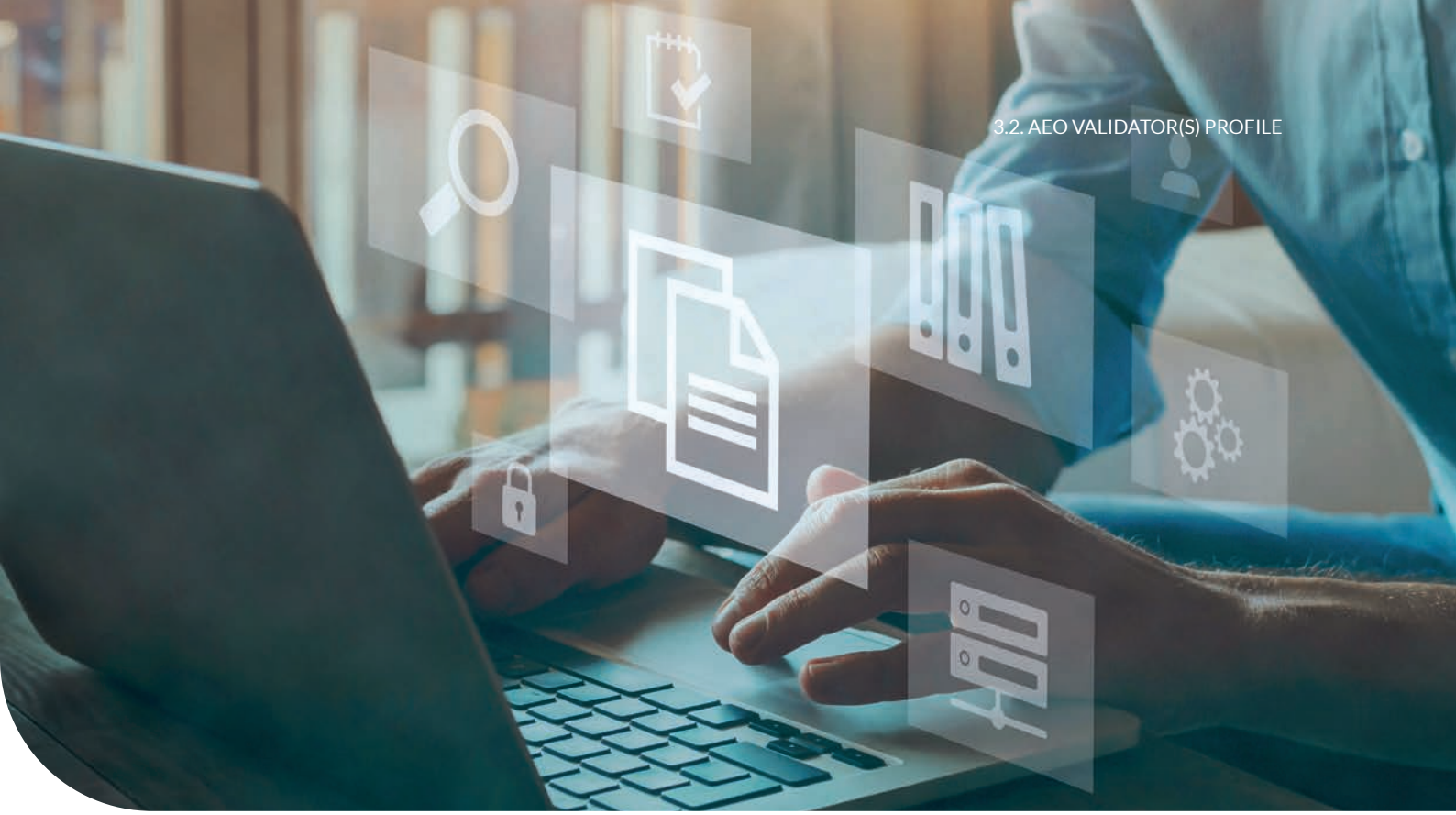
3.2.3. Validation competencies of AEO Validators

The competence, knowledge, skills and experience of a Validator are essential. In order to achieve the necessary competencies, Customs administrations should put in place a structured training programme. This requires (in addition to the other competencies):

- Understanding internal control measures;
- Accounting and internal controls;
- Assessing the operator's risks in relation to the AEO criteria;
- Developing a validation plan/control plan;
- Performing controls; and
- Completing the validation, drawing conclusions and issuing a validation report.

3.2.4. External knowledge/ development

For Customs Validators and their team leaders (and the entire Customs administration), it is essential to be aware of what is happening within the external environment. This knowledge is needed in order to adapt and update professional skills, knowledge and working methods to meet new and rising challenges (e.g. recent trends in fraud, new auditing techniques, new legislation, new technologies, how international standards work, and supply chain security threats). Validators and their team leaders should consider enrolling in supply chain security training offered by internationally recognized security programmes, such as ISO, BASC and TAPA.



3.2.5. Role of AEO Validators

- Prepare for validation: collect and analyse information, assess related risks, prepare validation plan, etc.;
- Coordinate meeting agenda;
- Understand the business process;
- Conduct 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);
- Obtain and verify any supporting documentation;
- Establish, record, observe, evaluate and test the applicant's procedures;
- Use the respective validation report templates;
- Complete a report covering the checks carried out and the conclusions that are drawn;
- Recommend whether the authorization should be granted or refused;
- Be available to advise the company throughout the process; and
- Whenever a compliance and/or security issue arises, make the EO aware of the importance of instructing and training employees to inform the Customs administration and other relevant authorities, where applicable.

Note: the knowledge, competencies and roles of Validators covered in paragraphs 3.2.2 to 3.2.5 are non-exhaustive and could vary, based on national or regional needs and differences. Customs administrations are encouraged to undertake the necessary training and development for their AEO Validators, as well as identify new areas that would be useful for the administration of the member's AEO programme.

3.3. AEO Validation – General Principles

3.3.1. Acceptance procedure for the AEO application

Economic operators (applicants) are in the best position to prepare their application for AEO status and should be guided by the AEO Self-Assessment Questionnaire (SAQ)/AEO template.

The SAQ, which contains questions addressing the qualification criteria (A to M), also includes general questions which allow the Customs administration to gather sufficient information to form a comprehensive view of the entity and identify any risks in its international supply chain. Customs administrations should be readily available to answer any questions from the applicant in order to help the latter complete the application process.

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

If additional information is required, the Customs administration must request it from the applicant as soon as possible, within the deadline provided for in legislation or national provisions, where applicable.

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

3.3.2. Risk analysis as a cornerstone in the evaluation process

Once an application has been accepted, the AEO validation process will commence using an outcomes-focused approach. By specifying the desired outcome to be achieved concerning the risk in an applicant's international supply chain, the AEO process caters for a greater level of complexity in terms of different business models and roles. The Validator, therefore, needs to confirm that the desired outcomes are met against each qualification criterion (A to M) in the AEO SAQ. This approach 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 for, 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 analysis of the risk and the weighting of the risk are an initial and iterative process. The risk assessment process should be consistent for all validations in order to ensure comparable results between AEO applicants.

There are two aspects to be considered when assessing the significance of a risk: the likelihood that an event will occur, and its potential impact. When considering the likelihood of an event occurring, it is necessary to take into account any existing measures or controls that are designed to mitigate the relevant risks.

The risk and threat assessment should cover all potential risks, including those of relevant government agencies, concerning AEO status, bearing in mind the role played by the economic operator in the international supply chain. The assessment should cover all the AEO criteria (A-M), including:

- Security/safety/health threats to premises, persons and goods;
- Customs and fiscal risks;
- Reliability of information related to Customs operations and logistics in respect of the goods;
- IT security and access to data;
- Reliability and competence of the operator's employees;
- Visible audit trail and prevention and detection of fraud and errors;
- Security/safety of business partners in the international supply chain.

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

Validators have the responsibility of planning and performing the validation in a way that addresses all potential risks. Therefore, the Validators need to verify compliance, safety and security in terms of criteria standards A to M. In this context, Customs' role is also to assess how effectively the economic operator manages the critical risks. In addition, Customs need to ascertain whether the measures the EO takes are adequate to reduce the risks to an acceptable level.

An applicant 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 of failing to meet the AEO criteria.

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 that are designed to mitigate the risks.

3.4. Validation Procedures Using a Holistic Approach

To identify the risks and prepare an effective and efficient validation, Validators must:

Understand the business entity and its organizational structure through the following non-exhaustive list:

- The Self-Assessment Questionnaire (Chapter II);
- Other 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, the internet, companies' annual financial reports, Validator's report on internal control, etc., and via communication with chambers of commerce and Central Statistics; certifications from non-profit organizations focused on supply chain security certifications (for example, ICAO, IMO, UPU, ISO, BASC, TAPA and others).

Understand the business organization through the following non-exhaustive elements:

- Partners operating in the international supply chain;
- External service providers and the impact of their role/activity on the applicant's international supply chain;
- Logistic processes executed in the applicant's international supply chain;
- Internal procedures relating to all the activities forming part of the international supply chain;
- Nationally recognized industry groups, trade associations and chambers of commerce.

Assess risk factors:

- Prioritize the risks identified, having analysed their impact on Customs objectives and the likelihood of the risk materializing;
- Assess to what extent the operator has taken measures to identify and mitigate risks, and in what way the operator has prioritized the different types of risk. The company's risk assessment document should be signed by a senior company official with authority to take appropriate action to mitigate identified 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:

- Take into account, to the extent allowable within a national AEO regime, national and international (security) programmes based on internationally recognized standards such as those of ICAO, IMO, UPU, ISO, BASC, TAPA and others.

Develop a validation work plan:

It is the responsibility of Validators to plan and perform the validation to obtain reasonable assurance that the economic operator is compliant with the established criteria. Validators should determine their work plan according to the risks identified for the economic operator/applicant in question. Only Customs administrations have the authority to grant AEO status. However, it is acceptable for Customs administrations to be guided by conclusions provided by third-party experts in relevant fields related to AEO requirements.

Visits to the facility must be communicated and coordinated in advance with the applicant's primary point of contact to ensure, among other things, that appropriate personnel and subject-matter experts are available for the validation process. The EO should be requested to have the most senior company official in attendance at the start of the meeting. Key business partners of the EO should be encouraged to attend and, if applicable, so too should representatives from the company's certifying organizations (for example ICAO, IMO, UPU, ISO, BASC, TAPA and others). The validation plan should be developed as a result of the risk assessment, and should reflect information about:

- The risks of each criterion outlined in the SAQ, indicating the relevant points/aspects to check;
- The management and staff members who are to be interviewed;
- The management and staff members from service providers and/or trading partners who are to be interviewed;
- What, how and when a specific transaction/security test should be done;
- The validation meeting agenda.

The AEO programme is formally built on a differentiated trust-based framework, providing economic operators who meet or exceed interna-

tional supply chain security and trade compliance standards with benefits at borders (point of entry and exit). These qualifying economic operators will be assessed as low-risk and benefit from reduced regulatory border and streamlined Customs processes.

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

3.4.1. Types of validation

Depending on the requirements and/or circumstances of each Member, any of the following three approaches can be followed when conducting the AEO validation:

Physical validation (on-site): performing a physical validation offers the greatest opportunity to understand holistic client architectures. It can involve running live tests and scenarios, inspecting premises and processes, and questioning clients on practical aspects of operations and risk implementation. On-site validations should be the first type of validation method to be considered when assessing an AEO applicant.

Virtual re-validation (remote): the expectation is that virtual re-validations can support risk management of the supply chain, whilst reducing the administrative burden. This approach does not replace all face-to-face Customs validations on-site. Rather, it allows Customs to perform relevant verification activities in an efficient and practical manner when a physical verification is (for whatever reason) not possible or desirable. It should not be utilized for new applicants unless the Customs administration and the AEO applicant feel comfortable with its capabilities.

Hybrid approach: with many AEO applications, the most appropriate process is combining a physical and virtual validation method. This hybrid approach can serve as a useful tool to (1) complement traditional validations, (2) provide a viable option to help manage "the next crisis", and (3) increase the reach of programmes (for example, when it is necessary to validate the processes of a business partner located at some distance from AEO staff).

The following section provides additional context on the importance of each method and how it complements the risk-based process, explaining the respective benefits of on-site and virtual validations in broader terms. This explanation is vital since, as technology and digital processes evolve and improve, so too do the capabilities of the applicant. Furthermore, as more economic operators are validated, Customs administrations' validation teams and techniques will also improve and mature.

a. Physical validations (on-site)

The validation documentation provides information that allows the Validators to reach the conclusions upon which their advice on approval or rejection of the application will be based. It can take several forms, most notably: documented procedures and instructions, verbal information (for example from an interview), information from observation, physical information and analytical information.

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

A guiding principle is that the goal of the validation should be not only to validate adherence to AEO requirements, but also to identify best practice that can be shared with other EOs. Furthermore, suggestions can be offered to the EO that will strengthen the applicant's security policies, procedures and practices in adequately addressing relevant risks in the applicant's international supply chain.

For evidence to be relevant, it should support validation findings and conclusions, and should be consistent with the objectives of the validation process. It should also be credible, by being factual, adequate and complete. Reliable evidence is achieved through the use of appropriate validation techniques. These should generally be selected in advance, and may be expanded during the validation work.

The Validators must fully capture or reflect the evidence in the validation report in order to substantiate the opinion reached, and to allow independent evaluation of the validation carried out.

b. Virtual validations (remote)

The advent of COVID-19 in 2020 has acted as a catalyst for business innovation, increasing the utilization of modern technology and a change in business culture. These developments have highlighted the opportunity to formally apply virtual validations in Customs and trade-related policies and processes to improve efficiency both for traders and Customs administrations.

Customs administrations and AEO companies operate in environments that are full of risks which could significantly disrupt normal operations. There are risks from natural disasters, pandemics, civil unrest, terrorism, fires and explosions, as well as a host of other threats. These risks are becoming commonplace within the context of the breadth and scale of operations of global businesses.

Appropriately identifying and planning for the above disruptions to normal operations are requirements under AEO programmes. So, it is expected that AEO companies devote the necessary resources to developing systems, training personnel, and creating a culture to manage business disruptions. It follows that Customs administrations should likewise be prepared to respond to threats on how to manage their AEO programmes and maintain the necessary oversight of AEO companies.

For the above reasons, Customs administrations should develop contingency plans that include processes to conduct virtual AEO validations when traditional in-person validations cannot be conducted.

The expectation is that virtual validations can support risk management of the supply chain, whilst reducing the administrative burden. The intention is not to replace all face-to-face Customs validation which takes place on-site but, rather, to perform the relevant verification activities in the most efficient and practical manner.

AEO programmes should incorporate a risk assessment methodology into the decision-making process on how Customs identifies which AEO companies could be validated virtually. Customs administrations should assess indicators such as the complexity of the AEO company's supply chain (number of business partners along the supply chain, how many of those business partners are AEO-certified, etc.); and the presence of terrorist or drug trafficking organizations. Cognizance must be taken of the AEO company's history of cargo disruptions (such as evidence of tampering, cargo theft, or contraband introduction), and factors such as the type of entity that needs to be validated. It is a lower risk for Customs to virtually validate a Customs broker than to virtually validate a highway carrier – the weakest link in the supply chain.

In this context, the addition of a range of virtual validations to the AEO toolkit will enable AEOs and Customs administrations to respond to threats to AEO activities more rapidly. These threats are especially relevant, given the obligation for Customs to manage AEOs' safety and security status, both at a national level and under international mutual recognition obligations.

Lesson Learned – Practical consideration

The text above explains that Customs administrations can consider a physical validation (on-site), a virtual validation (remote) or a hybrid approach to the AEO applicant validation process. This consideration is also addressed later under "Re-Validation" in Section 3.6.

Since virtual validations (remote or a hybrid) are still in their infancy, some early practical experiences can be shared, which may assist Customs administrations that are considering this validation approach.

The remote or hybrid validation process depends on technology, and so this approach will require more planning and time. Many potential pitfalls exist, most notably, videos often getting frozen, muted participants, and unstable connections which hamper proceedings. Additionally, the discussions tend to be limited to the official questions and answers. Furthermore, more specifically, virtual validation of security measures often requires additional planning on the part both of the Validator and the AEO applicant, since security measures are exceptionally complex when conducted virtually.

Despite these challenges, some remedies do exist, such as:

- Dividing the virtual validation into multiple phases, which could include a preparatory phase and virtual interview;
- Customs could provide in advance any questions related to the Self-Assessment Questionnaire;
- Administrative arrangements should be agreed in advance to prepare for any interruptions.

To facilitate the validation process, applicants should allow the Validator to have access to any available internal audit reports, and use live video delivery on cargo and premises security.

More follow-up meetings are needed when the Validator instructs the AEO applicant to make corrective actions, to validate that these actions have indeed been implemented.

Customs administrations should evaluate and document the challenges and lessons learned in order to help inform future enhancements to the virtual re-validation process.

3.5. AEO Validation Using the AEO Self-Assessment Questionnaire from Chapter II

The objective of the validation is to determine whether the applicant meets the AEO criteria, by assessing the effectiveness of the procedures and measures taken by the EO to address relevant risks. Participation in the AEO programme is voluntary and will allow entities such as importers, exporters, Customs brokers, freight forwarders and transport companies to nominate themselves to take part. This approach provides flexibility as it allows several matters to be taken into account.

These include:

- Role of the entity;
- Operations of the entity;
- Types of goods handled;
- Location of entity's operations;
- Size of the entity;
- Number of partners involved in its international supply chain.

All of these matters need to be taken into account when deciding whether the entity satisfies the relevant criteria. For example, an importer who imports "dangerous goods" would be expected to have different physical security measures to those of an entity who produces avocados.

Therefore, the validation should focus on the risks related to AEO requirements in general, as well as the specific activity/activities that the applicant is performing in the international supply chain.

Examples of validation testing techniques and other items of useful information are provided in the "Validators' corner" boxes below to assist the Validator with each criterion. The information provided in the Validators' corner is not exhaustive, nor does it represent a checklist of mandatory elements, but is merely provided as a guide.

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

The following section of this chapter corresponds to the overarching criteria (A to M) of the SAQ in Chapter II, addressing each specific sub-criterion and its associated Explanatory Notes. The layout of the SAQ is designed to help the applicant get a better understanding of the AEO programme, as well as to encourage voluntary participation. By specifying the desired outcome to be achieved in relation to potential risks in an applicant's international supply chain, the SAQ provides applicants with detailed guidance and caters for a greater level of complexity than did previous versions, in terms of different business models and roles. The Validator must confirm that the desired outcomes are met against each qualification criterion (A to M) in the SAQ.

The risk analysis principles outlined in Section 3.3, together with the overall validation requirements of Section 3.4, should help to provide the Validator with a good understanding of the validation task, when read in conjunction with the specific conditions relating to each criterion outlined below.

A. Demonstrated Compliance with Customs Requirements

This criterion requires the applicant to demonstrate a satisfactory level of compliance with national Customs-related laws and to have an effective system in place for quality assurance of Customs declarations. The criteria are to be fulfilled by the applicant, or by designated persons.

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.

In cases where the applicant has been established for less than the period determined by the national AEO programme, the Customs administration will assess compliance with the above criterion, based on the records and information that are available to it.

The record of compliance with Customs legislation may be considered to be satisfactory if the Customs administration competent to take the decision believes an infringement to be of minor significance in the context of the number or size of the applicant's operations, and if the Customs administration believes the applicant is acting in good faith.

Minor infringements are those acts that are not considered to pose a significant risk to the security of the international supply chain or Customs compliance, including revenue compliance.

In the event of infringements which could initially be considered as minor or being of minor importance, the Customs administration should establish whether there has been a repetition of infringements that are identical in nature. If so, the Customs administration should analyse whether that repetition is the result of the action of one or several particular persons within the applicant's company, or if it is the result of systemic deficiencies in the applicant's systems or procedures.

Following initial identification of the minor infringement, the Customs administration should monitor whether the infringement continues to occur. Alternatively, the Customs administration should detect whether the cause of the infringement has been identified by the applicant and appropriately addressed, meaning that it will not happen again in the future. Applicants should be able to demonstrate an effective system in place for quality assurance of Customs declarations to avoid future infringements. If, on the other hand, the infringement continues to occur, 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 concerning security or safety and/or Customs compliance.

Serious infringements could also be those that, even where the applicant has not intended to commit fraud or other breaches of Customs law, are so significant as to be considered a serious risk to supply chain security and/or Customs compliance, and where applicable, tax rules and criminal activity relating to their 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 related 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, etc.;
- Direct or indirect involvement in terrorist activities.

The criteria must ensure that circumstances relating to any previous non-compliance are put into context when assessing whether the requirements are met.

Validators' corner – validation testing techniques for demonstrated compliance with Customs requirements

- To identify whether the applicant and designated persons have 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 and designated persons have committed any serious criminal offences related to their economic activity.
- To examine detailed statements on any overdue or unpaid taxes or Customs duties with Customs and verify the appropriate channel or contact point to address any arrears in Customs duties/tax.
- To verify the effectiveness of the system to ensure quality assurance of Customs declarations.

B. 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. The applicant should also allow validation-based Customs control and maintain a historical record of data that enables the user to trace data from the moment it enters the data system to the time it leaves.

The records kept by the applicant for Customs purposes should be integrated into the accounting system of the applicant or should allow cross-checks of information against the accounting system to be made.

The applicant should allow the Customs administration physical and/or electronic access to its accounting systems and, where applicable, to its commercial and transport records. The applicant should have a logistics system which identifies the location of the goods. The criteria set out the baseline capability requirements for the applicant's operating systems (whether manual or electronic). The applicant's operating systems may include information technology systems or physical record-keeping systems. Processes and procedures may also form part of the entity's operating system.

The applicant should have administrative arrangements that are suitable for effectively managing the supply chain, and internal controls capable of preventing, detecting and correcting errors and of preventing and detecting illegal or irregular transactions. The essential element for the security of the international supply chain and for ensuring compliance with Customs-related laws is accurately recorded information that can be verified and traced to its source.

The applicant should employ adequate information technology security measures which will protect commercial records against access by unauthorized persons.

Validators' corner – validation testing techniques for satisfactory system for management of commercial records

- To ensure the company has satisfactory procedures in place for the archiving of its records and information, and for protection against the loss of information (i.e. maintenance of record-keeping systems).
- To determine whether the company maintains timely, accurate, complete and verifiable records relating to import and export.
- To ensure Customs has access to the company accounting systems and, where applicable, to its commercial and transport records.
- To ensure records are kept for the purposes both of Customs and the company's accounting system (whether it is integrated or not) and cross-check against the actual operations.
- To make transaction tests and ensure there is an internal trail in the records capable of tracing all transactions in the applicant's international supply chain that can be readily traced from the record or information.

C. Financial Viability

Financial viability means good financial standing which is sufficient to fulfil the commitments of the applicant (i.e. the entity is to be able to pay all its debts as and when they become due and payable), with due regard to the characteristics of the type of business activity and current economic conditions.

Any indication that the applicant is, or may in the immediate future, be unable to meet its financial obligations must be carefully considered and evaluated.

The applicant's financial viability is an essential indicator of their ability to maintain and improve measures to secure their supply chain and comply with other Customs requirements.

Validators' corner – validation testing techniques for financial viability

- To determine if the applicant has fulfilled (during a specific or assessment period) their financial obligations regarding payments of Customs duties and all other duties, taxes or charges relating to the importing or exporting of goods. Financial indicators may be utilized to identify the financial standing of the operator.
- To determine if the applicant has proven financial standing to meet their obligations and fulfil their commitments, by assessing records and information available for a specific period before applying.
- To determine if the applicant is subject to bankruptcy proceedings.

D. Consultation, Cooperation and Communication

Customs-to-Business Partnerships require contact points to be established for both parties, with a mechanism to engage both parties in an open and continued mutual exchange of information, where legally acceptable.

The applicant has an obligation, through the POC, to notify the appropriate Customs contact point in a timely manner of any unusual or suspicious cargo documentation, and of any emergency reporting and contingency planning involving goods for Customs purposes. This obligation can include any abnormal requests for information on shipments which is discovered by employees and is of interest to Customs administrations (cargo bookings, cargo tracking, employee information, etc.) or to any other relevant authorities.

Validators' corner – validation testing techniques for consultation, cooperation and communication

- To verify if the applicant has formally designated a POC to contact Customs for all Customs compliance and enforcement matters.
- To assess if the POC is thoroughly knowledgeable about the trade entity's practices and procedures and the AEO programme requirements.
- To ensure that the POC is empowered to provide the validation team with direct or indirect access to all information in a timely and accurate manner throughout the validation process.
- To ensure that the POC provides the appropriate access to all relevant places and personnel necessary to conduct the validation.
- To request written evidence that the applicant has implemented measures to notify the Customs administration of any AEO compliance issues.
- To ensure that the POC notifies Customs of the applicant's emergency reporting and contingency plans.

E. Education, Training and Threat Awareness

The applicant is required to have mechanisms in place for educating and training personnel regarding security policies and regarding recognition of deviations from those policies. There should be a clear understanding of what actions must be taken in response to security lapses. Relevant training may relate to the security measures, procedures and policies an applicant has in place to ensure the integrity of the international supply chain.

The applicant should have a security plan and a security awareness programme in place that prepares employees to handle a crisis or security breach that could interrupt operations, with the goal of:

- Ensuring business continuity and reactivation of the entire security system;
- Ensuring that incidents are appropriately investigated and analysed to identify areas for improvement;
- Developing procedures to report an incident or a risk situation to the Customs administration;
- Ensuring that staff are well informed of the details of the security plan, in order to take timely and appropriate remedial measures to respond to security threat scenarios;
- Educating personnel and business partners regarding the risks in the international supply chain, and conducting proper staff training to acquaint them with the contingency measures.

Validators' corner – validation testing techniques for education, training and threat awareness

- To request evidence of implementation that confirms that the applicant has established and maintains a security training and threat awareness programme.
- To request a list of the 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 test if security awareness and knowledge are disseminated in the company in order to assess the effectiveness of the training programme.
- To test the identification of risks in suspicious goods, potential internal threats to security, and to assist employees and contractors in protecting access control.

F. Information Exchange, Access and Confidentiality

The applicant is required to have adequate procedures in place for the archiving of records and sensitive information, including protection against the loss of this information. The applicant must also have appropriate security measures in place to protect the applicant's computer system from unauthorized intrusion, and to secure the applicant's documentation.

This criterion relates to information exchange, access and confidentiality. It requires the appropriate procedures to be in place to ensure all information communicated concerning the clearance and reporting of the goods is legible, complete and accurate, and is protected against the exchange, loss or introduction of erroneous information, including procedures to protect information from misuse and unauthorized access.

Validators' corner – validation testing techniques for information exchange, access and confidentiality

- To request policies and written procedures/evidence of implementation confirming that the applicant has IT security and archiving systems in place.
- To establish who is responsible for managing IT and IT security.
- To verify if the IT systems are accessed by individually assigned accounts (e.g. username and accompanying passwords).
- To verify segregation and extent of duties (e.g. different user profiles connected to the different tasks of the users).
- To verify which users have access to master data (such access should be very 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 and what the frequency of change is, if applicable.
- To request evidence of implementation that confirms that the economic operator has employee training that covers IT security policies, procedures and standards.
- To inquire if the applicant 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 applicant takes appropriate actions against employees that abuse/violate the IT systems.
- To establish that the applicant's IT server room is secured, and verify that only authorized employees/IT personnel have access to it.
- To establish that the applicant has a system in place to back up and store off site, on a periodic basis, critical data relevant to Customs and the AEO programme.

G. Cargo Security

Security measures should be in place to ensure that the integrity of cargo is maintained, and that irregular practices relevant to the flow of goods (transportation, handling and storage of cargo) in the international supply chain are prevented. Where appropriate to the business concerned, these measures should incorporate:

- Senior management's support for a supply chain security programme (written statement of support) and a proper oversight component (audit process in place to ensure that rotocols implemented by the company are being followed and are still viable);
- A procedure to ensure that the integrity of cargo units (including usage of seals and 7-point inspections (outside, inside/outside doors, right and left side, front wall, ceiling/roof, floor/inside, etc.) is maintained;
- Written procedures that stipulate how seals are to be controlled and affixed to cargo and transport conveyances (including procedures for recognizing and reporting compromised seals);
- Logistics processes (including choice of freight forwarder and means of transport);
- Incoming goods (including checking of quality and quantity, where appropriate);
- Storage of goods (including stock checks); and
- Production of goods (including quality inspections) and packing of goods (including the information on the packaging).

Criteria G, H, L and M require an applicant to undertake regular assessments of the security risks in its operations and to take appropriate measures to mitigate those risks. An applicant is required to satisfy each criterion, but only to the extent that the benchmark is relevant to the activities undertaken by the applicant in the context of its international supply chain.

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

Validators' corner – validation testing techniques for cargo security

- To verify that the information related to merchandise/cargo is legible, complete, accurate, and protected against unauthorized exchange, loss or introduction of erroneous information.
- To verify that security and control procedures are maintained to ensure that it is difficult for an unauthorized person to gain access to cargo, or for an authorized person to move, alter or interfere with the cargo improperly.
- To confirm that the EO verifies the physical integrity of the container structure, and that once loaded/stuffed following this inspection, the container is immediately sealed with an ISO 17712 high-security seal.
- To ensure the reliability of the locking mechanisms of the doors (e.g. 7-point container inspection).
- To ensure that container inspections are documented, and that the container inspection checklist may be requested to verify the information being captured.
- To witness a live container inspection and visually verify the secure storage of high-security seals that are being used by the applicant.
- 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, trained employees have access to high-security seals.
- To request, if possible, that the validation team witnesses 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.
- To verify how goods are protected against unauthorized access to storage facilities.
- To verify that the applicant has a procedure to ensure that cargo at time of loading matches the purchase order or other shipping document.
- To verify that the applicant has a procedure to identify that drivers arriving to pick up cargo are authorized by the transportation company.

H. Conveyance Security

Documented measures should be in place to ensure the integrity of cargo during its conveyance (transportation, handling and storage of cargo) in the international supply chain. Where appropriate to the business concerned, these measures should contain:

- Assurance that all transport conveyances used for the transportation of cargo within its supply chain are capable of being effectively secured (with a detailed procedure to be followed to preserve the integrity of cargo while in its custody);
- Logistics processes (including choice of freight forwarder and means of transport);
- Assurance that all operators used are trained to maintain the security of the transport conveyance at all times;
- Written procedures to report any actual or suspicious incident to designated security department staff, both of the AEO and Customs, for further investigation, as well as to maintain records of these reports, which should be available to Customs, to the extent legal and necessary;
- Notifications to Customs of any unusual, suspicious or actual breaches of transport conveyance security;
- Written commitment from the carrier to notify the company in a timely manner of any security breaches, unauthorized stops or deviations from established routes, so that the EO can make a determination as to whether to notify Customs or take other action to prevent a future recurrence.

Validators' corner – validation testing techniques for 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 cargo during the transport conveyance thereof.
- To verify procedures are in place to ensure the data on the transport documents matches the actual cargo (i.e. through well-documented handover points in the conveyance of cargo, coupled with a well-defined reconciliation procedure as a control).
- To verify procedures that manage, secure and control cargo conveyance while loading into or unloading from the transport conveyance, and during storage.
- To verify procedures are in place to ensure that goods are secured against unlawful or unauthorized movements, alterations or interference during movement of the goods into or out of the premises. This verification includes procedures while the goods are stored on those premises (goods in storage, separate storage for dangerous goods or high-value goods, stock-taking, and inventory procedure). All transport conveyances are to be checked for security breaches if left unattended.
- To ascertain what the escalation protocol is and who is responsible in the event of finding a concealed or suspicious good.
- To verify whether information is in place on real-time tracking (and whether there exists central visibility) of exported goods.

I. Premises Security

This criterion requires applicants to have physical security measures in place, which may include fencing, gates, lighting, alarm systems, video surveillance systems, locking devices, the structure of buildings on the premises, procedures for parking, etc.

In addition, security measures should be in place to prevent unauthorized access to offices, shipping areas, loading docks, cargo areas and other relevant places, in order to secure access to the premises and to prevent tampering with goods. The applicant needs to ensure that procedures are in place which monitor and control the exterior and interior perimeters and prohibit unauthorized access to facilities, transport conveyances, loading documents and cargo areas which may reasonably affect the security of its areas of responsibility in the supply chain.

All security-sensitive areas must be protected against unauthorized access by personnel and third parties who do not have the appropriate security clearance to access those areas. Procedures include access control of unauthorized persons, and of unauthorized vehicles and goods.

Where appropriate to the business concerned, these measures should include:

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

Validators' corner – validation testing techniques for 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 areas are protected against unauthorized access by staff and/or third parties.
- To verify how the EO manages the issuance and retrieval of identification badges to prevent misuse.
- To verify if the facility has perimeter barriers which are sufficient and also being maintained to deter/prevent unauthorized access.
- To verify if the buildings are constructed of materials that resist an unauthorized entry, and are maintained by periodic inspection and repair.
- To verify whether all internal and external windows and doors of the business premises are equipped with locking devices.
- To verify if adequate lighting inside, outside and throughout the entire premises is in place.
- To verify, where appropriate, the use of back-up generators or alternative power supplies to ensure constant lighting during any disruption to local power supplies.
- 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 cameras, alarm systems and any other access control system.
- To verify procedures relating to the use of vehicles on an applicant's premises, in order to prevent vehicles from being used in a manner that could impact the security of goods or containers.
- To verify who is in charge of monitoring the security measures and ensuring that the prescribed procedures are properly executed.

J. Personnel Security

The criterion requires reasonable precautions to be taken when recruiting staff, in order to verify that they have not previously been convicted of security-related Customs or other offences. These precautions will include background checks of employees working in security-sensitive positions (to be conducted periodically, or as and when they are needed). Additional measures will consist of procedures to remove identification from employees whose employment has been terminated, and to remove their access to premises and information systems. The screening processes may include pre-employment verification and background checks.

Security measures should be in place to prevent the hiring of individuals who could pose a security threat. The main areas that should always be 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 positions related to incoming/outgoing goods and storage; and
- The policy and procedures when staff leave 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, for the purposes of safety and security, the applicant should apply similarly appropriate measures to these other parties as it does to its business partners.

This criterion requires employee identification procedures in order to identify, record and deal with unauthorized and unidentified persons, and sign-in registers for visitors and vendors at points of entry.

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 check current employees periodically, and that third-party recruitment processes have similar screenings in place.
- To verify, to the extent legally possible, whether and how background checks of prospective employees are conducted (e.g. criminal, drug testing, financial, social-economic, etc.).
- To confirm that the EO has procedures in place to remove identification, facility and IT system access from employees whose employment has been terminated.
- To verify the denial of access for applicant former employees and contractors to the applicant's premises or systems, unless permitted by the applicant.

K. Trading Partner Security

The requirement to satisfy the qualification criteria must take account of diverse business models and roles in the international supply chain. This criterion will include business models where business partners and third parties may be engaged to undertake an activity that forms part of the entity's international supply chain. In some business models, the entity may have direct control over all activities in its international supply chain, whereas in other business models, there may not be such direct control.

Security measures should be in place to allow the applicant to identify the business partners. Additional measures should be in place to ensure, through the implementation of appropriate contractual arrangements or other appropriate measures, that those business partners ensure the security of their part of the international supply chain. This section is necessary to ensure the security of the applicant's international supply chain and trade compliance practices where the applicant does not undertake all the activities that form part of its international supply chain.

Therefore, when entering into contractual arrangements with a business partner, the applicant should, if necessary, take steps to ensure that the other contracting party assesses and enhances their supply chain security.

Additionally, the risk and responsibility of EOs and their trading partners should transfer from one party to another, in line with the International Commercial Terms (Incoterms) published by the International Chamber of Commerce (ICC). This criterion also allows the entity's responsibility to other people to be specified, and limiting that responsibility for taking reasonable measures and complying with those measures.

Management of risk related to business partners is essential, and a procedure for the screening and selection of business partners is strongly recommended. Therefore, the applicant should retain supporting documentation in this regard, thus demonstrating its efforts to ensure that its business partners are meeting these requirements or have taken mitigating actions to address any identified risks.

Physical and documentation verifications of business partners should be conducted through on-site visits, security questionnaires and virtual reviews, using available technology.

To strengthen the international supply chain, the applicant should encourage eligible business partners to join the national AEO programme. In cases where the business partner is not eligible, the AEO should encourage the business partner to join an internationally recognized security programme, such as ISO, BASC or TAPA.

Validators' corner – validation testing techniques for trading partner security

- To verify the EO has written and verifiable processes for the selection of business partners and external service providers.
- To verify if and how the EO has taken appropriate measures to provide adequate evidence that the business partner can meet an acceptable level of security and safety standards (i.e. incorporation of security and trade compliance requirements within the terms and conditions of contract with the business partner or third party).
- To request 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.
- To verify whether the EO requires any current or prospective business partners to have obtained AEO status and/or to be part of any other internationally recognized security-based programme, such as ISO, BASC or TAPA.
- To determine whether prospective business partners are chosen based on their adherence to certain security rules and, where applicable, mandatory international requirements, and to determine whether there is a clause preventing further subcontracting.
- To verify whether loaded containers are inspected at the subcontractor's premises, the terminal or recipient premises, and that they have been properly sealed.

L. Crisis Management and Incident Recovery

AEO status has a vital role to play in the effective handling and response to crisis management and incident recovery, including plans for business continuity on the part both of Customs administrations and business. The foundation of trust in AEO programmes is an essential asset in this context, being equally valid in situations such as natural disasters, pandemics and systems outages, or other national or global emergencies which affect the movement of goods across borders.

AEO programmes can support effective crisis management in the following areas:

- AEO status can facilitate the flow of goods in the event that risk assessment **operations**, including electronic processes, are suspended, affecting the capacity of administrations to use risk assessment tools before the release of goods.
- Normal **communications** networks are often unavailable during crises, and AEOs can provide a network of trusted and validated business channels to facilitate communication among themselves, and with local and national Customs contacts.
- AEOs on the ground can provide timely feedback on the **consistency** of processes at ports, including the requirements of other government agencies which may be key to health, safety and security – this information can be considered authentic and is important to recovery.
- AEO history of compliance in **revenue assessment and collection** provides a way to move some processes away from the border and reduce immediate burdens on business. These strategies include mitigating some penalties, delaying payment of duties and taxes, scheduling of audit activities, etc., while assuring administrations of revenue security.

With the above in mind, the applicant should have a crisis management, recovery and security plan in order to minimize the impact of a disaster or security incident. The plan should include the action points describing the measures to be taken in the event of incidents, and should be regularly updated (review programme).

An applicant should have in place a contingency plan for system disruption, with satisfactory procedures for the archiving of the company's records and information, and 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 exists, whether it includes action points describing the measures to be taken in the event of incidents, and whether it is regularly updated. In addition, any back-up routines when computer systems do not 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 in place and maintains a security recovery plan that reactivates the security system within a minimum time period.
- To verify how incidents are investigated and 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 administration if a security breach has occurred or a potential threat scenario exists.
- To verify how the EO educates personnel and, if appropriate, business partners, concerning inherent and residual international supply chain risks and corresponding mitigation strategies.

M. Measurement, Analyses and Improvement

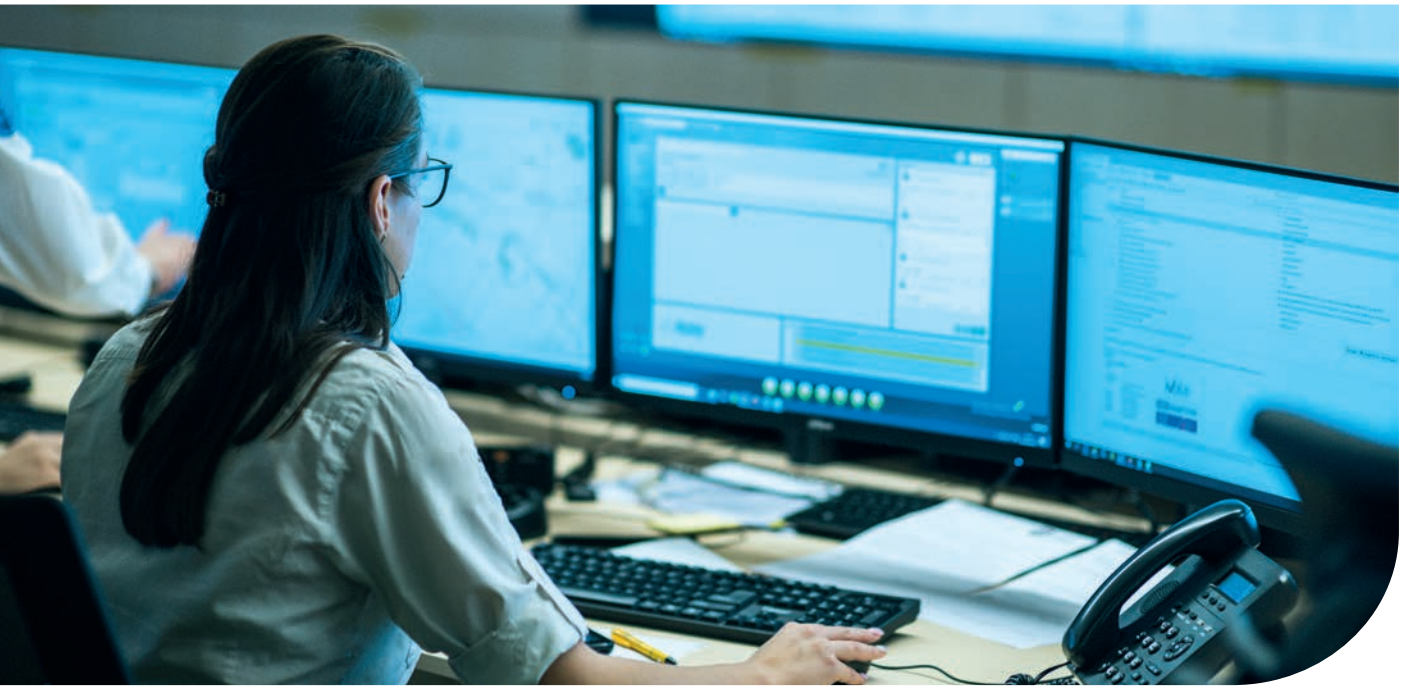
The applicant is required to establish and conduct regular self-assessments of its security management system, and fully document the self-assessment procedure and the responsible parties.

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 feedback from the designated parties and recommendations for possible enhancements in the review assessment results, incorporating these recommendations in a plan for the forthcoming period to ensure continued adequacy of the security management system.

Validators' corner – validation testing techniques for measurement, analyses and improvement

- 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 in place plans for continued improvement, as well as validation planning.
- To verify that the improvement measures recommended have been taken effectively (follow-up).
- To provide recommendations on further improvements, based on security assessment reports, where applicable.



3.6. Reporting and Follow-Up

3.6.1. Reporting

Validators should ensure that the analysis of findings includes:

- 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 fulfilment of the AEO criteria;
- A clear description of all risk areas considered and checked, and any follow-up actions suggested to the applicant;
- A clear report of any action or reaction the applicant has undertaken or expressed to the Validator;
- A clear recommendation about whether to grant AEO status or not, according to the result of the 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 AEO status is not granted, complete and detailed justifications as to why this is the case;
- 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 to reflect the overall work already carried out (risk analysis, validation planning, checks and visits to the premises of the applicant, the risk profile of the specific economic operator, etc.), doing so in a summarized and systemised way and clearly indicating future actions.

The final report should include the documentation relating to supply chain vulnerabilities and best practice found throughout the validation process.

3.6.2. Follow-up of AEOs

Monitoring

Once AEO status is granted, one has to differentiate between monitoring and re-assessment. Monitoring is done continuously by Customs administrations, in the context of Customs-to-Business (C-2-B) Partnerships, to understand, facilitate and, where appropriate, to inspect and regulate the activities of the AEO (which may include visits to its premises).

Monitoring aims at the early detection of any areas for improvement, so that appropriate corrective actions can be taken to help the AEO improve. Where serious non-compliance is detected, monitoring also supports the investigation and other regulatory actions that need to be taken, including re-assessment, suspension or revocation, as the case may be.

The ongoing monitoring of the AEO is a joint responsibility of the AEO itself and of the Validator or responsible Customs representative. Nevertheless, regular monitoring is the primary responsibility of the economic operator and should form part of its internal control systems. The economic operator should be able to demonstrate how the monitoring is performed and to show the results.

Likewise, monitoring is done continuously by the Customs administration, and should include maintaining an open dialogue with the AEO to ensure that the AEO is made aware of newly identified risks/trends or programme updates. Any 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 are key in enhancing the partnership approach to maximize supply chain security and trade facilitation.

Re-Assessment/Re-Validation (on-site)

Re-assessment may imply that serious non-compliance issues have been detected and that action has to be taken 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 confirm continued compliance with the AEO criteria and suggest potential measures for enhanced compliance.

In addition, a re-assessment is required if there are changes in legislation specific to, and having an impact on, the conditions and criteria related to AEO status.

Virtual/Re-Validation (remote)

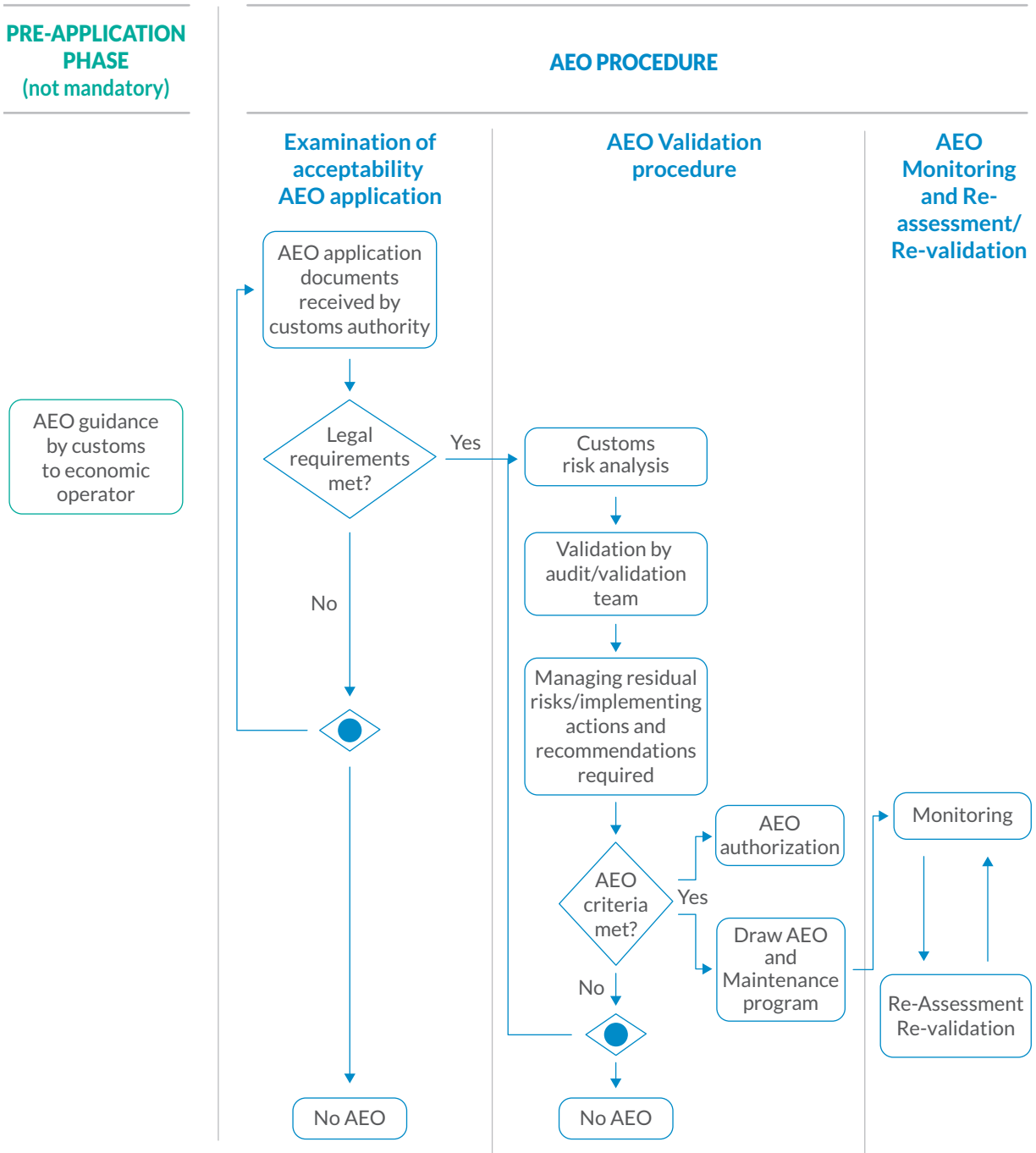
The adoption and use of virtual re-validation can be especially relevant to the management of AEO programmes, where the emphasis is on the AEO and Customs to develop a mutually beneficial relationship. That relationship is based on the establishment of high-quality business practices that enable the company to consistently manage risk and demonstrate its compliance with AEO regulations. The utilization of technology and virtual re-validations can enable Customs and other regulatory agencies to receive specific, relevant and timely information that can act as material evidence relevant to the AEO. This utilization can support the Customs-AEO relationship during application, verification, service and the provision of benefits, monitoring, or re-verification activities.

Virtual re-validations can enable Customs to efficiently review or assess trader risk remotely, in real-time, or potentially, by enabling the creation of a material audit trail of evidence or records for future verification. The table below identifies some of the potential benefits to Customs, OGAs and AEOs.

Speed and flexibility	Integrity	Costs
Provides potential for real-time Customs/OGA-Business engagement and resolution.	Provides an expanded auditable trail of evidence.	Removes non-critical travel and meeting times for Customs and the client.
Enables a single submission for control purposes, for use by one or numerous regulatory authorities.	Reduces risk of potential for patronage or syndication.	Builds relevant verifications into the AEO/client's business process, saving time.

APPENDICES

Appendix I - AEO Flow-Chart



Appendix II - EU Best Practice on Auditors and Economic Operators

This appendix is not a comprehensive checklist, but an indicative tool to help operators and Validators manage their AEO programme.

Threats, Risks and Possible Solutions

This document provides a list of the **most significant risks related to the AEO** authorization and monitoring process. 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 may apply 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, the type of goods, type of automated systems, and level of modernization of the operator.

The "Threats, Risks and Possible Solutions" 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 and origin; - use of Customs procedures; - taxation rules; - application of measures 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 of Customs requirements.	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 timeliness of transactions, and disclosing irregularities/errors, including suspicion of criminal activity, to Customs administrations. Procedures to investigate and report errors found, and to review and improve processes. The competent/responsible person within the business should be clearly identified, and arrangements for holidays or other types of absence should be in place. Implementation of internal compliance measures. Use of audit resources to test/ensure that procedures are correctly applied. Internal instructions and training programmes to ensure staff are aware of Customs requirements.	

2. The applicant's accounting and logistical system

Criterion: A satisfactory system for managing commercial and, where appropriate, transport records, which allows appropriate Customs controls.

2.1. Accounting system

Indicator	Risk description	Possible solutions	References
Computerized environment Integrated accounting system	The risk that an accounting system is inconsistent with the generally accepted accounting principles applied in the Member State. Incorrect and/or incomplete recording of transactions in the accounting system. Lack of reconciliation between stock and accounting records. Lack of segregation of duties between functions. Lack of physical or electronic access to Customs and, where appropriate, transport records, breaching the auditability. Inability to readily undertake an audit due to the way in which the applicant's accounting system is structured. Complex management system offers possibilities to cover up illegal transactions. No historical data available.	Segregation of duties between functions should be examined in close correlation with the size of the applicant. For example, in a micro-enterprise which conducts a road transport business and has a small number of everyday operations, the packing, handling and loading/unloading of goods might be assigned to the driver of the truck. However, the receipt of the goods, their entry in the administration system and the payment/receipt of invoices should be assigned to another person(s). Implement a warning system which identifies suspicious transactions. Develop an interface between Customs clearance and accounting software to avoid typing errors. Implement enterprise resource planning (ERP). Develop training and prepare instructions for the use of the software. Allow cross-checks of information.	ISO 9001:2015, section 6

2.2. Audit trail

Indicator	Risk description	Possible solutions	References
Audit trail	The absence of an adequate audit trail mitigates efficient and effective audit-based Customs control. Lack of control over the system's security and access.	Consultation with the Customs administration prior to the introduction of new Customs accounting systems to ensure they are compatible with Customs requirements. Testing and ensuring the existence of the audit trail during the validation phase.	ISO 9001:2015, section 6
Mix of Customs-cleared goods, and goods not Customs-cleared	Lack of logistical system which distinguishes between Customs-cleared goods and goods not Customs-cleared. Substitution of Customs-cleared goods, and goods not Customs-cleared.	Internal control procedures. Data entry integrity checks to verify if the data entries are correct.	

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, and for unauthorized 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 person responsible for quality to be in charge of the company's procedures and internal controls. Make each head of department fully aware of the internal controls of their own department. Record the dates of internal controls or audits, and take steps to correct identified weaknesses. Notify the Customs administration if fraud, or if unauthorized or illegal activities, are discovered. Make the relevant internal control procedures available to the personnel concerned. Create a folder/file in which each type of goods is linked to its own Customs information (tariff code, Customs duty rates, origin and Customs procedure), depending on the volume of goods concerned. Appointment of a person(s) responsible for managing and updating the Customs regulations applicable (inventory of regulations), and for updating data in the enterprise resource planning (ERP) software and clearance/accounting software. Inform and educate staff regarding inaccuracies and how they can be prevented. Have in place procedures for recording and correcting errors and transactions.	ISO 9001:2015, sections 5, 6, 7 and 8

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 on relevant staff and submission of declarations as scheduled. Records of stock movements. Regular stock reconciliations. Arrangements for investigating stock discrepancies. Ability 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 in 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. Formalization of procedures for import. Perform regular inventories. Perform punctual consistency checks on 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 in the accounting records.	Persons are appointed to authorize/ oversee the sale/release process. Formalization 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 the declaration in cases involving Customs 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. 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 administrations about identified irregularities in compliance with Customs requirements.	Implement formal procedures to manage/follow each Customs activity and formalize specific clients (classification of goods, origin, value, etc.). These procedures are intended to ensure Customs Department continuity in the event 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 to fill in the declaration and documents to produce). Implement procedures for notification of any irregularities to Customs administration.	ISO 9001:2015, section 6

Representation through third parties	Lack of controls.	Routines should be implemented to check work of third parties (e. g. on Customs declarations) and to identify irregularities or violations by representatives. 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 is necessary for the declarant to determine the tariff (technical specifications of goods, samples, etc.). If externalization of the exportation of goods by an approved exporter applies, the outsourcing can be committed to a Customs agent allowed to act as the authorized 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 licence's validity and registration. Segregation of duties between registration and internal controls. Standards for reporting irregularities. Procedures to ensure the use of goods is 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 from 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 licences as per individual requirements; to ensure there is awareness training/education for staff dealing with goods with non-fiscal aspects.	

2.7. Procedures as regards back-up, recovery, 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-up routines. Lack of satisfactory procedures for the archiving of the applicant's records and information. Deliberate destruction or loss of relevant information.	The presentation of an ISO 27001 certificate demonstrates high standards in IT security. Procedures for back-up, recovery and data protection against damage or loss. Contingency plans to cover systems disruption/failure. Procedures for testing back-up and recovery. Customs archives and commercial documents saved in secure premises. Presence of a classification scheme. Adherence to archival legal deadlines. Back-ups should be done daily, on either an incremental or full basis. Full back-ups should be done at least once a week. A minimum of three latest consecutive back-ups should be available at all times. Back-ups are preferably done remotely, through an electronically secure method at a storage facility located at least 300 metres away. Encryption key should also be backed up and stored away from the storage facility.	ISO 9001:2015, section 6 ISO 27001:2013 ISO norms for standards in IT security

2.8. Information security – protection of computer systems

Indicator	Risk description	Possible solutions	References
General	Unauthorized access to and/or intrusion into the economic operator's computer systems and/or programmes.	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, or identification of issues relating to IT risk. Procedures for granting access rights to authorized persons. Access rights are to be withdrawn immediately on transfer of duty or termination of employment. Access to data on a need-to-know basis. Using encryption software where appropriate. Firewalls. Anti-virus protection. Password protection on all PC stations and possibly on important programs. If employees leave their work station, the computer should always be secured via keyword. Password should consist of at least eight characters and include a mix of two or more upper-case and lower-case letters, numbers and other characters. The longer the password, the stronger it is. Usernames and passwords should never be shared. Testing against unauthorized access. Limit access to server rooms to authorized persons. Perform intrusion tests at regular intervals; intrusion tests are to be recorded. Implement procedures for dealing with incidents.	ISO 27001:2013

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 rights. Procedures to inhibit the use of personal consumer ware, such as pen drives, CDs, DVDs 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 authorized access to documents. Filing and secure storage of documents. Procedures for dealing with incidents and taking remedial action. Recording and back-up of documents, including scanning. Contingency plan to deal with losses. Possibility to use encryption software if needed. Commercial agents to be aware of security measures while travelling (never consult sensitive documents in transport). Set up access levels to strategic information, according to different categories of personnel. Handle discarded computers in a secure manner. Arrangements with business partners for protection/use of documentation.	ISO 28001:2007, section A.4 ISO 27001:2013
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 are 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 organization	Inadequate coordination of 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 of view. Implement procedures to ensure security and safety of goods in the event of holidays or other types of absence 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 for security and 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, sections 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, counter-measure, and signature of the responsible person. Make the register of security and safety incidents available to employees of the company.	ISO 28001:2007, sections 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 and goods	Unauthorized access or entry of vehicles, persons or goods to the premises and/or close to the loading and shipping area.	The number of vehicles with access to the premises should be as limited as possible; for that reason, parking for staff should preferably be outside the security ring. In addition, if possible, trucks should be 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 loading. The use of badges is reasonable. The badges should have a photo on them. If there is no photo on the badges, they should at least indicate the name of the operator or the premises where they are valid (risk of misuse if 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 times. Data on all entries, including names of visitors/drivers, arrival/departure times and attendants, should be recorded and stored in appropriate form (e.g. logbook, IT system) and 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; standardized procedures for the return of all access authorizations. Visitors should be met and supervised by the business to prevent any unauthorized activities. Identification badges for visitors have to be worn visibly. Speak to unknown persons. Corporate clothing to recognize unknown persons. In cases involving temporary work (i.e. maintenance work), a list of authorized workers of the outsourced company.	ISO 28001:2007, section A.3 ISPS Code

Standard operating procedures in case of intrusion	No proper action if intrusion has been discovered.	Implement procedures for cases involving intrusion or unauthorized entry. Conduct intrusion tests, 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 unauthorized 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 authorized personnel only are adequately signed and controlled. Irregular patrols of the security staff.	ISO 28001:2007, section A.3 ISPS Code
Gates and gateways	Existence of gates or gateways which are not monitored.	All gates or gateways in use should be secured through appropriate measures, i.e. CCTV and/or entry control system (lighting, beamers, etc.). CCTV is only useful when the recordings can be evaluated and can allow reactions in real-time. 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.	Instructions/procedures on use of keys are in place and available to staff concerned. Only authorized personnel have access to keys to locked buildings, sites, rooms, secure areas, filing cabinets, safes, vehicles, machinery and air cargo. Conducting periodic inventories of locks and keys. Log attempts to gain unauthorized access, and check this information on a regular basis. Windows and doors should be locked when nobody is working in the room/ office.	ISO 28001:2007, section A.3

Lighting	Inadequate lighting for external and internal doors, windows, gates, fences and parking areas.	Adequate lighting inside and outside. Where appropriate, the use of back-up generators or alternative power supplies to ensure constant lighting during any disruption to local power supplies. Plans in place to maintain and repair equipment.	
Procedures for access to keys	Lack of adequate procedures for access to keys. Unauthorized 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 use. The return of keys must also be registered.	ISO 28001:2007, section A.3.3
Internal physical security measures	Inappropriate access to internal sections of the premises.	Implement a process to distinguish between the different categories of employee on the premises (i.e. jackets, badges). Access is controlled and personalized according to employee position.	ISO 28001:2007, sections 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 unauthorized entry of private vehicles to protected areas. Specific rules/procedure for entry of private vehicles onto the applicant's premises. In cases when there is a non-separate parking area for visitors and employees, cars of visitors should have an identification.	
Maintenance of 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 of 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. Unauthorized 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 area monitored by security personnel), or other measures are taken to ensure the integrity of the cargo unit. Access to the area where cargo units are held is restricted to authorized 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 and checking the integrity of cargo units. Procedures for recording, investigating and taking remedial action when unauthorized access or tampering has been discovered. Where appropriate, monitoring via CCTV.	ISO 28001:2007, section A.3.3 ISPS Code
Use of seals	Tampering with cargo units.	Use of container seals that are compliant with ISO/PAS 17712 or another appropriate type of system ensuring the integrity of cargo during transportation. Seals stored in a secure location. Register of seals (including used seals) is maintained. Regular reconciliation between register and seals held. Where applicable, make arrangements with business partners to check the seals (integrity and numbers) on 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. Incomplete control of the cargo units.	Procedures to examine the integrity of the cargo unit prior to loading. Where appropriate, use of 7-point inspection process (front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage prior to loading). Other types 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 afterwards.	ISO 28001:2007, section A.3
Standard operating procedures in case of intrusion and/or tampering with cargo units	No proper action if unauthorized access or tampering has been discovered.	Appropriate procedures laid down on what measures should be taken when unauthorized access or tampering is discovered.	ISO 28001:2007, 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 on 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 may pose a security or safety risk.	Maintain a schedule of expected arrivals. Procedures for handling unexpected arrivals. Perform consistency checks between incoming goods and entries in the logistics systems. Procedures for testing the integrity of the means of transport.	ISO 9001:2015, section 6.2.2 ISO 28001:2007, section A.3
Routines for verifying security measures imposed on others	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	Procedures for ensuring staff are aware of security requirements. Management/supervision checks to ensure that security requirements are complied with.	ISO 28001:2007, section A.3
Supervision of 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 of 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/airmail from a known consignor: have appropriate systems and procedures in place to check 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 safety risk. Introduction, exchange or loss of received goods.	Procedures to check the integrity of seals and that the seal number corresponds to the number in the documents. Appointment of designated authorized person.	ISO 28001:2007, section A.3 ISO/PAS 17712

Administrative and physical procedures for the receipt of goods	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	Checks to compare the goods with the accompanying transport and Customs documents, picking lists and purchase orders. Checks on completeness by weighing, counting and tallying, and checks on the uniform marking of goods. Updating stock records as soon as possible on arrival. Goods representing an anomaly placed in a specific and secure area, and a process created 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 or broken anti-tampering devices, including the review of procedures and taking of 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. One or more areas are designated for the storage of goods, with a CCTV surveillance system or other appropriate controls.	
Goods to be stored outdoors	Manipulation of goods to be stored outdoors.	Need for use of adequate lighting and, if appropriate, CCTV surveillance. Integrity of these goods has to be checked and documented before loading. If possible, show the destination of these goods at the latest possible stage (i.e. barcodes 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 stock-taking, and for recording and investigating any irregularities/discrepancies, including the review of procedures and taking of remedial action. Instructions regarding goods notifications, addressing how and in what way the incoming goods will be checked.	ISO 9001:2015, section 2
Separate storage of different goods	Unauthorized 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 and air cargo) are stored separately.	TAPA (Technology Asset Protection Association) Certificate
Additional security and safety measures for access to goods	Unauthorized access to the goods.	Authorized access to the storage area for designated staff only. Visitors and third parties should have temporary identification badges and be accompanied at all times. Data on all visits, including names of visitors/third parties, arrival/ departure times and attendants, should be recorded and stored in appropriate form (e.g. logbook, IT system). If own storage area is on another operator's premises, that area should be secured by regular communication between the operators involved, and by spot visits and controls 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. Unauthorized access to the goods.	An area is designated for production of goods, with appropriate access controls. Authorized access to the production area for designated staff only. 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. Tampering with the goods.	Security processes and procedures should be established to ensure the integrity of the production process, e.g. authorized access for designated staff or appropriately authorized persons only, supervision and monitoring of the production process by systems and/or personnel.	ISO 28001:2007, section A.3
Packing of products	Incomplete control over the packing of the products. Introduction, exchange or loss of produced goods.	Wherever possible, products should be packed in a way that allows tampering to be detected easily. An example could be the use of special tape with brand names on it (in which case the tape has to be kept under supervision). 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 these goods at the latest possible stage (i.e. barcodes instead of plain text indicating destination).	
Quality inspection	Incomplete control over the flow of goods. Introduction, exchange or loss of produced goods.	Conduct 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 safety risk.	Control the goods loaded against the information from logistics departments (consistency checking/counting/ weighing/loading list/sales order). Check with the logistical system that procedures are in place on reception of means of transport. 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 have no control.	Procedures for ensuring staff are aware of customer's security requirements. Management/supervision checks to ensure that the security requirements are complied with.	ISO 28001:2007, section A.3
Supervision of loading of goods	Lack of supervision of loading of goods which might pose a security or safety risk.	Checks on completeness via 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 conduct checks on routines.	ISO 28001:2007, section A.3
Sealing of outgoing goods	Sending out goods that are not sealed can lead to introduction, exchange or loss of goods which cannot easily be discovered.	Procedures for controlling, applying, checking and recording seals. Appointment of designated authorized person. Use of container seals that are compliant with ISO 17712 for high security seals.	ISO 28001:2007, section A.3 ISO 17712

Administrative processes for the loading of goods	Delivery of goods which is not registered in a logistical system and of which you have no control, 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 of 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 anti-tampering devices, or customer returns, and to 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 company-specific certification (which can be set up on the basis 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 (e.g. through the use of internet or rating agencies) used to select regular business partners. Security requirements (e.g. that all goods must be marked, sealed, packed and labelled in a certain way, or subject to X-ray checks) are written into contracts with regular business partners. Requirement that contracts will not be further subcontracted to unknown third parties, particularly for the transportation of secure air cargo/ airmail. Conclusions provided by experts/ external auditors who are not related to regular business partners, on compliance 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. Reporting and investigating any security incidents involving business partners, and recording remedial action taken.	ISO 28001:2007, section A.3

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 for unspent convictions). Requirements on staff to disclose other employment, police cautions/ bail, pending court proceedings, and convictions. Periodic background checks/re-investigations for current personnel. Removal of computer access, and return of security pass, keys and/or badge when staff leave or are dismissed. Checks on temporary staff applied to the same standard as for permanent staff. Contracts with employment agencies detail the level of security checks required. Procedures to ensure employment agencies comply with those standards.	ISO 28001:2007, section A.3
Level of safety and security awareness of personnel	Lack of proper knowledge of security procedures related to different processes (incoming goods, loading, unloading, etc.), with the consequence of accepting/loading/ unloading unsafe or insecure goods.	Staff awareness of security measures/ arrangements related to different processes (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 noticeboard. Display the security and safety rules in the relevant areas (loading/unloading areas, etc.). The signs must be visible internally (on the sites) and externally (dedicated places for drivers, temporary workers and various partners).	ISO 28001:2007, section A.3

Security and safety training	Lack of mechanisms for training employees on safety and security requirements and, consequently, inadequate awareness of security requirements.	Persons responsible for identifying training needs, ensuring delivery, and keeping training records. Training employees to recognize potential internal threats to security, detect intrusion/tampering and prevent unauthorized access to secure premises, goods, vehicles, automated systems, seals and records. Conducting tests with respect to "unsafe" goods or occasions. Security and safety training can be part of industrial safety training aimed at all staff. Security and safety training has to be documented and updated regularly (e.g. every year), based on actual situations which have arisen in the company. New staff should receive intensive training, given their lack of knowledge and awareness.	ISO 28001:2007, section A.3

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, or restricted access controls) are written into contractual agreements. Monitoring of compliance with these requirements. Use of different badges for external staff. Restricted or controlled access to computer systems. Supervision of external services, where appropriate. Establish security arrangements and/or auditing procedures to ensure the integrity of the goods. In cases involving temporary work (i.e. maintenance work), a list of authorized workers of the outsourced company.	ISO 28001:2007, section A.3

Appendix III – Best Practices

a. Best practices framework

https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/bestpractices

b. Examples of risk mapping models

US
http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/ctpats-five-step-risk-assessment.pdf?la=en,

EU
http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/eu_aeo_compact_model.pdf?la=en,

Brazil
http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/brazil_aeo_risk_management.pdf?la=en

Appendix IV – Examples of Financial Viability Indicators

4.1. The European Union

List of methodological indicators to demonstrate sufficient financial standing

The Customs authorities can establish whether the applicant is able to meet his/her legal debts to third parties by checking the applicant's full sets of financial statements due over the past three years, taking into account:

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

4.2. China

Suggested indicators for the financial viability and sustainability evaluation of enterprises during the validation process

During the validation of an enterprise, the first step should be to make sure that the Finance Department's procedural document is in place and is appropriate. In addition, the accounting documents and account books as well as the accounting statements should provide true, accurate and complete records. The processing of the accounts should conform to accounting standards. At the same time, an unqualified audit report by an accounting firm is required.

In order to evaluate the enterprise's financial solvency, we use the **quick ratio** and **asset-liability ratio.** The certified enterprise's quick ratio and asset-liability ratio must be within a safe and normal range.

In order to evaluate the enterprise's profitability, we use the **profit margin of costs and expenses**. Likewise, the certified enterprise's profit margin of costs and expenses must be within a safe and normal range.

Additionally, we require evidence that the certified enterprise's **operating net cash flow** for the previous year is not negative (the number of years for which operating net cash flow is required retrospectively depends on the validation cycle of the relevant Customs administration). Given that cash flow indexes are much harder to manipulate than profit indexes, operating net cash flow is one of the most accurate indexes for describing an enterprise's operating situation.

In order to judge if the indexes are within a safe and normal range, we use the evaluation criteria published by the State-owned Assets Supervision and Administration Commission to assess the enterprise's performance.

We suggest using the annual average data when calculating the quick ratio and asset-liability ratio, as this data can denote the enterprise's performance over a period of time and not only at a given point in time.

Index	Calculation formula
Quick ratio	(Circulating assets - merchandise)/current liabilities x 100%
Asset-liability ratio	Total liabilities/total assets x 100%
Profit margin of costs and expenses	Total profit/total cost and expenses x 100% (total cost and expenses = operating costs + operating taxes and surcharges + selling expenses + management expenses + financial expenses)

4.3. The Eurasian Economic Union (EAEU)

AEO financial solvency criteria: financial indicators

	Absolute indicators
1	Net assets
2	Amount of charter capital
3	Residual value of fixed assets
	Relative indicators
4	Equity ratio
5	Liquidity adequacy ratio
6	Return on equity (ROE)
7	Financial stability ratio
8	Working capital financed by equity to total assets
9	Current assets to equity ratio

The Customs Code of the Eurasian Economic Union (hereinafter the "EAEU") stipulates financial stability as a condition for granting Authorized Economic Operator (hereinafter "AEO") status.

The Eurasian Economic Commission (hereinafter the "Commission"), together with EAEU Member States, has developed a methodology for determining the financial stability of potential AEOs.

This methodology was approved by the Council of the Commission on 15 September 2017.

This methodology document provides a unified algorithm for assessing the financial stability of potential AEOs, for Customs purposes. At the same time, this document is open to and available for business as well as for Customs authorities. It rules out a subjective approach to determining financial sustainability.

In total, there are nine indicators of financial sustainability. Three of them are absolute, expressed in national currencies. Six indicators are, however, relative and expressed as percentages (ratio).

Each indicator has a minimum value. Points are allocated when a company's parameters meet these minimum values. If the potential AEO reaches a calculated value exceeding or equal to the set value of a particular indicator, then it may be allocated a certain number of points. A company is not precluded from becoming an AEO if it has no points for a particular indicator. In such a case, the company may amass points for another indicator if its parameters exceed minimum values.

All points received must be totalled up and, if they exceed 50 points, then the applicant is considered financially sustainable for Customs purposes.

The financial solvency indicator values are calculated on the basis of the legal entity's annual accounting reports. The company's financial sustainability is subject to annual reassessment. If the company is considered as financially sustainable (i.e. if it meets the financial solvency criteria), then it does not need to provide a financial guarantee.

The above-mentioned suggestions are based on the new EAEU Customs Code that entered into force on 1 January 2018.

Contact us:
facilitation@wcoomd.org

Visit our website:
wcoomd.org

Acknowledgement: This publication was printed with the financial support of CCF-Korea
Photo credits: © Stock.adobe.com
Publication number: FAC 2021-2 – Legal deposit: D/2021/0448/10

World Customs Organization

Rue du Marché 30, B-1210
Brussels, Belgium
facilitation@wcoomd.org

#WCOOMD
wcoomd.org