AEO Eligibility and Requirements

Who is entitled?

- Any Economic Actor in the international supply chain
- Having dealing with Customs
- For example : manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors and freight forwarders

AEO Requirements

Eligibility criteria:

- Demonstrated Compliance with Customs Requirements,
- Satisfactory System for Management of Commercial Records,
- Financial Viability, and
- Security (cargo, conveyances, premises, personnel and trade partners).

Conditions & Requirements in the SAFE FoS

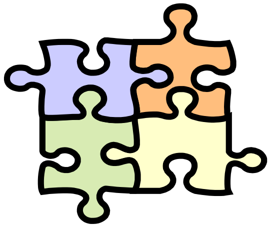
- Voluntary programme
- Flexibility and customization of security plans based on business model
- Phased Approach - step-by-step implementation

Customs administrations should not burden the international trade community with different sets of requirements to secure and facilitate international commerce. There should be one set of international Customs standards developed by the WCO that do not duplicate or contradict other recognized intergovernmental security requirements.

Approach of SAFE Framework

- Recognizes the complexity of international supply chains
- Endorses the application and implementation of security measures based upon risk analysis
- Allows for flexibility and customization of security plans based on an AEO's business model
- Lists certain Customs-identified best security standards and best practices
- One set of international Customs standards developed by the WCO that do not duplicate or contradict other recognized intergovernmental security requirements
- Reference to *Annex IV of WCO SAFE* and *AEO Template*

Annex IV of the SAFE structure



1. introduction
2. Definitions
3. Conditions and Requirements for Customs and the Authorized Economic Operator
4. Benefits to the Authorized Economic Operator
5. Validation and Authorization Procedure
6. Process outline for business involved in the handling of cargo within the international trade supply chain

SAFE ANNEX IV

1. Introduction

- “baseline” technical guidance for implementation
- Standards for both Customs and AEOs
- Various stakeholders are involved in the trade supply chain

Customs needs cooperation from Business

⇒ participation of business is fundamental to the success

- Transparency, predictability

⇒

- Conditions and Requirements
- Clear and tangible Benefits

2. Definitions

- Third party validator
- Validation
- Authorization
- Phased Approach
  - step-by-step implementation

3. Conditions & Requirements

- Introduction
  - Flexibility and customization of security plans based on business model
  - Best security standards and best practices

Customs administrations should not burden the international trade community with different sets of requirements to secure and facilitate international commerce. There should be one set of international Customs standards developed by the WCO that do not duplicate or contradict other recognized intergovernmental security requirements.

3. Conditions & Requirements

- **A. Demonstrated Compliance with Customs Requirements**
- **B. Satisfactory System for Management of Commercial Records**
- **C. Financial Viability**
- **D. Consultation, Co-operation and Communication**
- **E. Education, Training and Awareness**
- **F. Information Exchange, Access and Confidentiality**
- **G. Cargo Security**
- **H. Conveyance Security**
- **I. Premises Security**
- **J. Personnel Security**
- **K. Trading Partner Security**
- **L. Crisis Management and Incident Recovery**
- **M. Measurement, Analyses and Improvement**

A. Demonstrated Compliance with Customs Requirements

- Compliance history of a prospective AEO
  - Not have committed, over a period determined by the national AEO programme, an infringement/offence as defined in the national legislation
  - Infringements/offences under Customs Law and other laws
- Consider prospective AEO's procedures on Customs matters and routine
  - e.g. verifying the accuracy of Customs declarations, Customs valuation, tariff classification, ROO
  - e.g. training on Customs matters

B. Satisfactory System for Management of Commercial Records

- AEO shall:
  - Maintain timely, accurate, complete and verifiable records relating to import and export
  - Give Customs full access to necessary records, subject to the requirements of national legislation
  - Permit Customs to conduct any audit of cargo movements relating to import and export
  - Employ adequate internal records acces and control systems to protect against unauthorized access (ICT security)

C. Financial Viability

- AEO shall have good financial standing which is sufficient to fulfill its commitments with due regards to the characteristics of the type of business activity.
- AEO shall maintain and improve standards
  - e.g. Provide profit and loss statements and balance sheets
  - e.g. Declaration of insolvency proceedings
  - e.g. Statements from banks or financial institution or National Tax Bureau

D. Consultation, Co-operation and Communication

Customs and AEOs

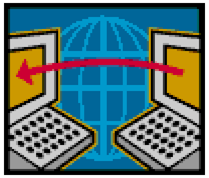
- Regular consultation
- Contact person (Customs Client Coordinator)
- Reporting

- Any unusual or suspicious-cargo documentation or abnormal requests for information on shipments
- illegal, suspicious or unaccounted cargo

E. Education, Training and Awareness

- Procedures in place:
  - To raise security awareness
  - To educate personnel with regard to the risks associated with movement of goods
  - To educate employees in maintaining cargo integrity, recognizing potential internal threats to security and protecting access controls
  - to identify and report suspicious incidents
- Educational material, manuals and appropriate training on the identification of potentially suspect cargo
- In-house training for AEOs and Customs personnel

F. Information Exchange, Access and Confidentiality



Customs and AEOs

- Full implementation of electronic data exchange
- Protection from misuse
- Sound data privacy and confidentiality

AEOs

- Legible, complete and accurate
- Protection from loss, exchange and error
- ICT policy: firewalls, passwords, backup

Customs

- Single Window
- Electronic procedures

Information and information technology security

- Information Security (broader concept)
  - Process of preserving the confidentiality, integrity and availability of *physical* and *electronic* data and *information systems*, including protection against the exchange, loss or introduction of erroneous information.
- IT Security
  - Putting in place measures to protect hardware, software, and network of an organisation from any disaster or external attacks (such as virus attack, hacking). It is more to do with *electronic* data
- May refer to ISO 27000 series for more details

Why is it important?

- Based on the *value* and the *consequences* of being compromised
- Type of information:
  - Financial information
  - Trade and research secrets
  - Proprietary business information
  - Employee data
- Consequences (can be very costly):
  - Huge financial penalties
  - Expensive law suits
  - Loss of reputation and business

Information security

- Confidentiality
  - ensuring that information is accessible only to those authorized to have access
- Integrity
  - safeguarding the accuracy and completeness of information and processing methods
- Availability
  - ensuring that authorized users have access to information and associated assets when required

Information Security

- Information Security Policy
- Procedures in place for:
  - Security classification of information
  - Access control of information
  - Data storage, backup, recovery, and disposal
  - Flagging out discrepancies (system capability)
- Awareness and training on info security for staff

Information technology (IT) and security procedures

- Procedures in place:
  - To maintain confidentiality and integrity of data and information systems used in the supply chain, including protection against misuse and unauthorized alternation
  - To ensure proper transfer, storage and final disposal of data and information
  - To determine access rights and protection for computer system

Accountability

- Segregation of functions between users and access controls to computer systems
- Procedures/systems in place to identify the detected abuse of IT including improper access, tampering or the unauthorized altering of business data
- Records of unauthorized access and measures taken to prevent recurrence, and any disciplinary actions

Data back-ups and recovery plans

- Main server and data back-ups
  - Where is it ?
  - How is it secured?
  - Frequency of data back-up
- Procedures in place for back-up capabilities to protect against loss of information
- Contingency plan for system disruption/failure

G. Cargo Security

- Putting in place procedures and processes to ensure the integrity of cargo by :
  - Having documented procedures and processes on cargo handling and storage
  - Having proper reporting mechanisms in place for cargo-related incidents
  - Having effective communication and training for personnel involved in the supply chain activities
- Security Policy
- Seal integrity (with ISO 17712 standard)
- 7 point inspection (conveyance & container)
- Access control

Why is it important?

- Ensure the integrity of cargo is not compromised
  - safeguard against tampering; involving removal of goods / placing of undesirable goods
  - safeguard against internal theft (ensure clear segregation of roles of personnel handling the cargo)
  - allow the investigation of cargo-related incidents in a systematic manner and implement corrective actions to prevent future lapses
    - e.g over/short landing of goods, damaged goods

Documentation processing and verification

- Procedures in place:
  - To ensure information in all documentation used in the movement and clearance of cargo, both electronic and manual, are legible, complete and protected against the exchange, loss or intentional introduction of erroneous information
  - Direct staff what should be done if they encounter a suspicious document

Receipt and release of cargo

- Procedures in place:
  - To ensure that arriving and departing cargo is reconciled against relevant documents
  - To compare the cargo with delivery documents when receiving and releasing cargo and to inform the appointed security officer if a discrepancy is detected
  - To ensure that persons/drivers delivering or receiving cargo are positively identified before cargo is received or released

Procedural documentation

- Procedures in place:
  - For critical process handover points (e.g. documentation preparation processes, issue of seals, breaking of seals, physical count of cargo, conveyance inspection, cargo delivery, cargo receipt)
  - Pertaining to custody and responsibility over cargo when a party takes receipt of the cargo or when a service is provided
  - To monitor on a continuous basis the movement of the cargo
  - For monitoring the loading of cargo for export

Container Inspection

- Procedures in place to verify the physical integrity of the container prior to stuffing, including the reliability of the locking mechanisms of the doors
- A 7-point security inspection process –
  - Front wall,
  - Left side, Right side,
  - Floor,
  - Ceiling/roof,
  - Inside/outside doors,
  - Outside/undercarriage

Container seals

- Procedures in place:
  - On how seals are to be controlled (received, stored, assessed, used and accounted for) and affixed
  - To ensure only designated authorised persons distribute seals
- Use ISO 17712 compliant high security seals

C-TPAT
Customs-Trade Partnership Against Terrorism
BUILDING PARTNERSHIPS • PROTECTING FREEDOM
ISO
International Organization for Standardization
TRANSBOLT

Storage of conveyances, containers and cargo

- Procedures in place to prevent unauthorized access and/or tampering of conveyances, containers and cargo in company’s custody stored in a secure area.

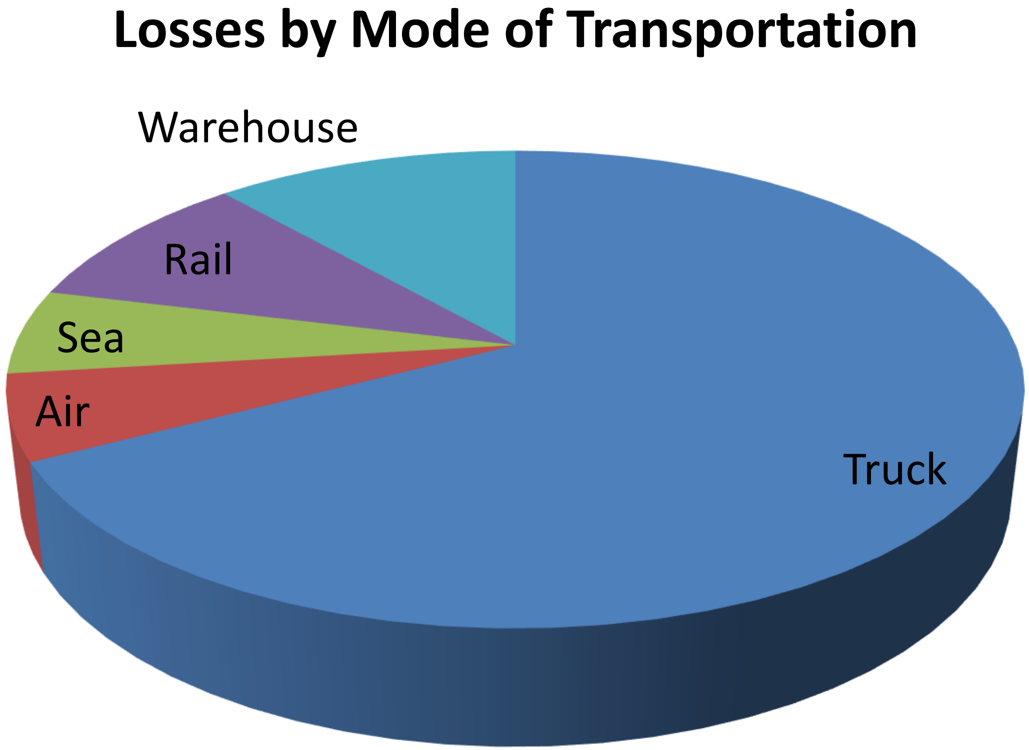
Storage sheds in Import warehouse equipment with high mast handling Cargo
bhadra

H. Conveyance Security

- Safeguarding the custody and integrity of cargo by establishing procedures to track and monitor accurately activities relating to the movement and handling of cargo both
- Security check after left unattended
- Regular check for concealment places
- Security awareness

Why is it important?

- Globally, some 80 % of all major cargo thefts occur during road transportation



Conveyance inspection

- Procedures in place to ensure that potential places of concealment on conveyances are regularly inspected
- Note that we are not referring to safety or cleanliness inspection but security inspection

Tracking and monitoring

- Procedures in place to track and monitor the movement of conveyance carrying the cargo between companies and external parties
- Can be done manually (e.g. two-way communication with the driver), semi-auto (e.g. RFID, barcode scanning) or auto (e.g. GPS, active e-seals)

Drivers’ guide

- Procedures in place to train drivers on:
  - Inspection of conveyance
  - Confidentiality of load, route and destination
  - Policy on keys, parking areas, refueling and unscheduled stops
  - Reporting for accident or emergency
  - Reporting of any irregularity in loading, locking and sealing
  - Testing of security alarms and tracking devices, if any

I. Premises Security

- AEO shall implement security measures and procedures to prevent unauthorised access to companies' facilities:
  - Perimeter fencing
  - Manned or monitored gates and exits
  - Parking
  - Building structure
  - Locking devices and key controls
  - Lighting
  - Alarm systems and video surveillance cameras
  - Security personnel and organisation
  - Access control for employees
  - Access control for visitors and vendors/contractors
  - Challenging and removing unauthorised persons

Why is this important?

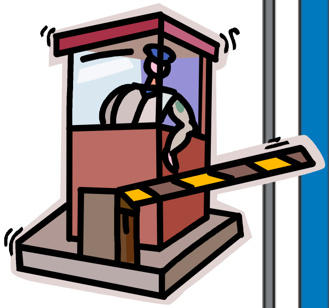
- Physical security serves as a first line of defense in protecting a premises.
- Although the security measures put in place may not 100% prevent the unauthorized access into the premises, they help the organization to *deter* and *delay* the offenders' actions and thus give the organization and/or security officers sufficient time to *react* and *respond*.
- Should deploy Prevention Strategy – Deter, Detect, Deny, Delay and Detain

Perimeter fencing

- Appropriate peripheral and perimeter barriers to enclose cargo handling and storage facilities
- Restricted areas should be clearly identified
- Procedures in place for:
  - Segregation of high value and hazardous cargo
  - Ensure that all fencing is regularly inspected for integrity, damage and repaired
  - Perimeters identifiable (signage) as controlled areas for authorized personnel only
- Other factors to consider: type, condition and height

Gate and gate houses

- Is it manned, monitored or controlled for vehicles and personnel?
- Procedures in place for:
  - Control the movement of all vehicles and personnel entering and exiting
  - Protect premises against unauthorized access by private vehicles
  - Specify when and how the searches of vehicles and personnel is conducted
- Only properly identified and authorized persons, vehicles and goods are permitted to access the facilities.



Parking

- Procedures in place:
  - To ensure that vehicles requiring access to restricted facilities are parked in approved and controlled areas
  - To prohibit the parking of employees and visitors' vehicles in close proximity to cargo handling and storage areas
- Parking access to facilities should be controlled and monitored

Building structure

- Constructed of materials that resist unlawful entry and protect against external intrusion
- Procedures in place to ensure the integrity of the structure is maintained by periodic inspection and repair
- Other factors to consider: all openings such as doors, windows

Locking devices and key controls

- Procedures in place:
  - To ensure that all external and internal windows, doors, fences and gates are secured with locking devices or alternative access monitoring or other control measures
  - For issuance and access to locks and keys
  - For conducting periodic inventory of locks and keys
- Management or security personnel must control the issuance of all locks and keys

Alarm systems

- Security systems such as intruder alarms, surveillance video recordings, lightings and access controls which are installed to deter, detect and delay offenders from their actions, are recommended to be integrated in an effective and coordinated manner
- Procedures in place:
  - Maintenance of equipment (sensors and alarm) and records
  - Testing of equipment
  - Alarm response plan

Video Surveillance cameras

- Should be used to monitor the premises and images should be useful to assist in post-incident investigations
- Procedures in place to maintain the equipment and retention of recordings
- Other factors to consider:
  - Strategic positioning of CCTVs throughout the facility
  - Maintenance of CCTVs
  - quality of recordings
  - storage of recordings
  - lighting

Lighting

- Procedures in place to ensure that adequate lighting inside and outside company facilities including
  - Entrances and exits
  - Cargo handling and storage areas
  - Fence lines
  - Parking areas

Security personnel and organization

- A personnel or unit must be in charge of the security of the company. Company may engage the services of a security organization to further enhance the security of their facilities
- Roles and responsibilities, and procedures put in place for and to review the personnel/unit/security organization

Access controls for employees

- Procedures in place:
  - To positively identify an employee and its access control
  - To deal with loss of pass or when access control is being compromised

- Employees should only be given access to those areas needed for the performance of their duties
- Employees should display their staff pass prominently at all times

Access controls for visitors and vendors/contractors

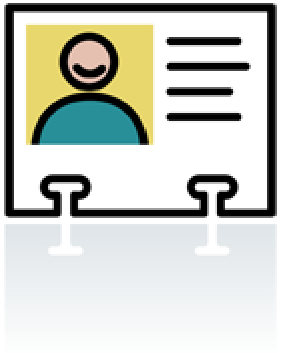
- Procedures in place to positively identify and manage access control for visitors and vendors/contractors
  - To register and control all visitors, vendors and contractors
  - To present photo identification or proper vendor ID
  - All visitors are required to visibly display identification passes
  - Visitors should be escorted if possible.

Challenging and removing unauthorized persons

- Procedures in place for employees to report and challenge unauthorized or unidentified persons
- Contingency plan deal with access by unauthorized persons

J. Personnel Security

- Putting in place processes and procedures to minimize the risk posed to the business operations by:
  - New hires
  - Current employees
    - Intentional
    - Unintentional
  - Terminated/resigned employees
- Background checks
- ID



Why is it important?

- Allowing security lapses or oversights in personnel security can be a very costly lesson to learn
- The cost to screen an employee is substantially less than the cost of security lapses due to failure to screen an employee
- Employees handle the company’s assets i.e. tangible (goods) and intangible (information)

Pre-employment verification and background checks

- Procedures in place:
  - To ensure the application information for both permanent and temporary personnel, such as employment history and references, verified prior to employment
  - To ensure background checks conducted on prospective permanent and temporary personnel as appropriate and to the extent allowed for by law

Periodic background checks/ reinvestigations for current personnel

- Procedures in place:
  - For the provision of periodic checks to the extent allowed by law performed on current permanent and temporary employees
  - As to whether the periodic checks are based upon the position and responsibilities of the personnel in the company

Resignation and termination of personnel

- Procedures in place:
  - To remove id cards, as well as premises and information systems access for terminated and permanent and temporary personnel
  - To control the employee’s ability to compromise security standards, if company policy, national law, employment contract or union agreement allows for a period of continued employment between termination/resignation notice and last work day

K. Trading Partner Security

- Encouraging trading partner (TP) to enhance security voluntarily
- Better written in contractual arrange

- Either outsource or contract elements of their businesses (e.g. conveyance, warehouse)
- Trading partners include current and prospective suppliers, manufacturers, service providers, contractors and vendors, customers

Why is this important?

- "A chain is only as strong as its weakest link"
- If any of its TPs does not have as good a system, then the opportunities for security breaches in the supply chain would arise
- Any security breaches would directly or indirectly impact the company
- Thus, it is important to select TPs who also practices security in their operations

Selection of Trading Partner

- Procedures must be in place for screening and selection of TP
  - Should include screening and selection criteria such as legality, financial solvency, supply chain security capability (relevant security certifications) etc
  - Conduct background checks, search denial lists
  - Cannot be solely based on cost, reputation, quality assurance

Security requirements for TP

- Procedures in place for TP to demonstrate they are meeting company’s supply chain security requirements e.g.
  - – State security obligations through contractual obligations
  - – Obtain written or electronic confirmation from senior management of TP
  - – Provide security profile/audit results/ relevant security certifications such as AEO certification

Review of TP's compliance to security requirements

- Procedures must be in place to monitor and review TP's compliance to security requirement e.g.
  - Conduct regular meetings with TP to review TP's compliance to security requirements, its KPIs etc
  - Perform security audits on TP
  - Review security audit results/certifications submitted by TP

L. Crisis Management and Incident Recovery

- To minimise impact of a disaster or terrorist attack
- Requires advance planning and establishment of processes to operate in extraordinary circumstances
- AEO and Customs shall:
  - Develop and document contingency plans for emergency security situations and for disaster or terrorist incident recovery
  - Should involve the appropriate authorities/parties where necessary
  - Conduct periodic training of employees and testing of emergency contingency plans.

Crisis management Plan

- Describes the various actions which need to be taken during critical situations or crisis
- Examples:
  - Natural crisis – earthquakes, tsunamis, volcanic eruptions
  - Pandemic - SARS, H1N1, Ebola
  - IT disaster
  - Industrial accidents, oil spills
  - Terrorism, espionage
  - Strikes
  - Kidnapping
  - Rumours

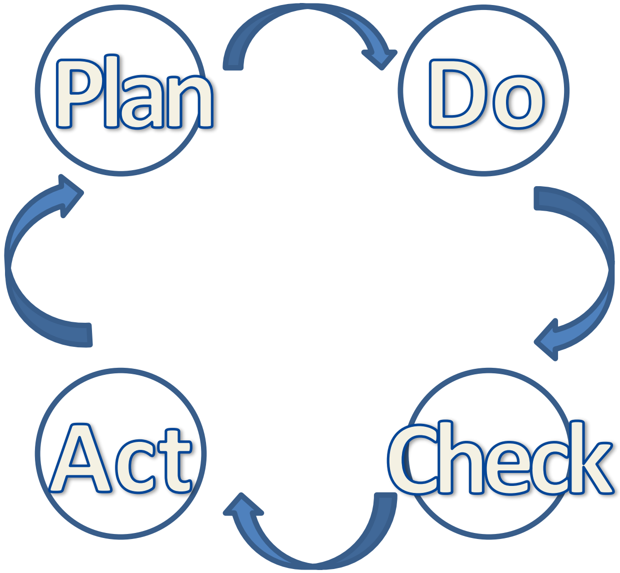
Trade continuity and resumption plan

- Consists of procedures and information for managing a disaster when it occurs
- Enables the continuation of company’s critical functions at an acceptable level
- Business operations can still continue
- Reduce financial and non-financial impacts
- Refer to ISO 22301 Business Continuity Management System for more info

M. Measurement, Analyses and Improvement

Monitoring, measurement, analysis and improvement

- Self-assessment, PDCA cycle
- Procedures in place:
  - To conduct assessment of the security risks in business operations and take appropriate measures to mitigate those risks
  - To establish and conduct regular self-assessments of its security management system
  - Fully document the self assessment procedure and the responsible parties with mechanism to include their feedback and recommendations



Points for Consideration

- No entry barriers e.g. minimum turn over, minimum no of declarations or duty paid
- Not to follow prescriptive approach
- Flexibility and customization of security plans based on the AEO’s business model
- Principle of proportionality
- Holistic and outcome based approach towards physical security requirements to assess overall adequacy of security requirements

Points for Consideration

- Baseline security standards based on unique operation environment and business model – lowers entry barriers (even for SMEs) while still ensuring compliance to security requirements

- Need for high level of training, professionalism, integrity and management oversight for a qualitative and objective assessment of security compliance

- Involvement of PGAs in the design and implementation of AEO programme

Authorized Economic Operators - SAFE FoS

Authorized Persons – RKC

Authorized Operators -WTO TFA

Customs Business Partnership
- Win -Win -

Customs

- Improved trade security
- Trade efficiency
- Effective enforcement
- Effective use of limited resources

Business

- Prompt customs clearance
- Lower transaction cost
- Transparency and predictability of procedures
- More business opportunity

Partnership

Government

- Economic and Social development

Authorized Person
- the RKC (GA 3.32) -

- Eligibility Criteria includes:
  - An appropriate record of compliance with Customs requirements, and
  - A satisfactory system of managing commercial records.

- Benefits:
  - Release of goods on minimum necessary information,
  - Clearance at the declarant’s premises or another place authorized by the Customs,
  - Single declaration for all imports/exports over a period,
  - Self assessment of duty and tax on the basis of commercial records,
  - Goods declaration by means of an entry in the records of the AP followed by a supplementary Goods declaration.

Authorized Economic Operator (AEO) – the SAFE FoS

- Eligibility criteria:
  - demonstrated compliance record,
  - satisfactory system for the management of commercial records,
  - financial viability, and
  - security concerning cargo, transport conveyances, premises, personnel and trade partners.

- Benefits:
  - benefit of entire government/country, Customs and Business

Government
- Improved revenue collection
- More FDI
- Coordinated Border Management

-> Economic development

Customs
- Efficient allocation of resources
- Streamlining requirements
- Driving Customs reform and modernization

Business
- reduced data sets for cargo release
- expedited processing and release
- minimum cargo security inspections
- reduction of/exemption from bank guarantees
- priority inspection
- reduction of theft and damage
- improved internal efficiency
- benefits from other countries – MRAs
- enhanced competitiveness and reputation

Authorized Operators
Article 7.7 of the WTO TFA - Broad features -

- Additional trade facilitation measures to ‘Authorized Operators’
- Specified criteria may include:
  - an appropriate record of compliance with customs and other related laws and regulations;
  - a system of managing records to allow for necessary internal controls;
  - financial solvency, including, where appropriate, provision of a sufficient security or guarantee; and
  - supply chain security.

- No criteria mandatory,
- No arbitrary or unjustifiable discrimination,
- No restriction to SMEs.

Trade Facilitation Measures

- Authorized Operators -

- At least three benefits of the following:
  - low documentary and data requirements,
  - low rate of physical inspections and examinations,
  - rapid release time,
  - deferred payment of duties, taxes, fees and charges,
  - use of comprehensive guarantees or reduced guarantees,
  - a single customs declaration for all imports or exports in a given period, and
  - clearance of goods at the premises of the authorized operator or another place authorized by Customs.

Comparison of AO, AP and AEO

	Authorized Operator	Authorized Person	AEO (SAFE FoS)
Program character	Business Partnership Program (should be developed together with business !)		
Base document	The WTO TFA - Article 7.7	The RKC - GA 3.32	The SAFE FoS (Customs to Business Pillar 2-Annex III)
Primary objective of the program	Trade Facilitation	Trade Facilitation (Simplification)	Supply Chain Security
Major requirements	• Good compliance record; • Commercial record management; •Financial solvency, including; and •supply chain security. (none of them mandatory)	Compliance requirements •Good compliance record •Commercial record management	Compliance requirements+ Security requirements •Premises security •Employee security •Cargo security etc
Benefits	•Clearance with info and reduced examination •Deferred payment of duties/taxes •Clearance at traders' premises , etc	• Clearance with minimum info • Clearance at traders' premises etc	• Reduced examination • Customs consultation point • Priority examination • Mutual Recognition, etc
coverage	Importer/Exporter	Importer/Exporter	Importer/exporter, transporter, customs broker, consolidator etc.

Analysis

- Benefits for AOs in the WTO TFA - similar to RKC and SAFE AEO
- Focus in AO is on trade compliance and supply chain security may be one of the component, while AEO must always comply with a range of security standards
- Specified criteria not mandatory- varied models of the scheme.
- The Authorized Operator (AO) could be an:
  - Authorized Person (AP) and/or
  - Authorized Economic Operator (AEO)
- SAFE AEO is more comprehensive
  - A more standardized and structured approach
  - A much wider dimension
  - Seamless Mutual Recognition Agreements

Analysis

- Para 7.5 of the Article 7.7 of the TFA foresees the possibility of negotiating mutual recognition of authorized operator schemes
- Challenge to have a common approach for MRA due to varied models of AO.
- Para 7.4 of the Article 7.7 of the TFA– use of international standards.

- If a Member successfully implements SAFE AEO, it complies with WTO TFA AO

FAQ on Linkages (similarities and differences) between SAFE AEO and Article 7.7 of the WTO TFA

1. Does implementing the SAFE AEO Programme fulfil the obligations of Article 7.7 of the WTO TFA?
2. Could programmes/schemes under the WTO TFA Article 7.7 be stepping stones towards eventual implementation of a fully-fledged SAFE AEO Programme?
3. What is the likely impact of Article 7.7 of the WTO TFA concerning AOs on existing AEO Programmes established by WCO Members based on the WCO SAFE FoS?
4. What is the likely impact of Article 7.7 of the WTO TFA concerning AOs on existing AEO Programmes established by WCO Members based on the WCO SAFE FoS?

How would mutual recognition of AO Schemes work?

Challenges

- Identifying tangible benefits
- Making fast clearance even faster
- Security validation - Customs officers are not trained
- Cultural shift from our traditional Customs control mindset to one of trust
- Adapting current processes and systems to meet the requirements of a Customs Compliance/AEO Programme
- Migration from compliance and facilitation programme to security and facilitation programme
- Engaging business and making them understand value proposition
- Necessary changes in law/regulations
- Involving all economic actors in the supply chain especially SMEs

Conclusion

- Examples of Members whose Customs Compliance Programmes are developed to AEO programmes
- Global trend that more and more Members consider AEO and Customs Compliance Programmes for benefit of entire government/country, Customs and Business
- Standardised approach to pave the way for maximising benefit of the entire supply chain and seamless mutual recognition
- AO could be a stepping stone for implementation of full fledged AEO
- Regional AEO programmes
- WCO's full support to its Members

Where is AEO going?

- ✓AEO and Post
- ✓AEO and E-commerce
- ✓AEO and Agriculture
- ✓AEO and Regulated Agent(RA)/Known Consignor (KC)
- ✓AEO and The International Ship and Port Facility Security Code (ISPS Code
- ✓AEO and Transport Asset Protection Association (TAPA)
- ✓AEO and Free Zone (FZ)
- ✓AEO and FIDI (largest global alliance of professional international moving and relocation companies)

Thank you for your attention!

Asha Menon

Asha.menon@customs.gov.my