

## **Threats, Risks and Possible solutions**

This document provides a list of the most significant risks related to the AEO authorisation and monitoring process, and at the same time, it provides a list of possible solutions on how to keep these risks under control. Possible solutions proposed for one indicator can be applicable to more than one risk area identified. The suggested list is neither exhaustive nor definitive.

The self-assessment questionnaire is completed by the economic operators at the very beginning of the application process and aims to give a state of play of their business and procedures and their relevance for the AEO authorisation. The ‘Threats, risks and possible solution’ document is addressed both to customs authorities and economic operators to facilitate the audit and examination to ensure compliance with AEO criteria by matching the information provided in the SAQ and the risk areas identified and possible solutions to cover them.

### **1. Compliance record (Section 2 from the SAQ)**

*Criterion: An appropriate record of compliance with customs requirements (Article 14h of CCIP)*

<b>Indicator</b>	<b>Risk description</b>	<b>Possible solutions</b>	<b>References</b>
Compliance with customs requirements	<p>Non-compliant behaviour with regard to:</p> <ul style="list-style-type: none"> <li>- fulfilment of customs declarations including incorrect classification, valuation, origin,</li> <li>- use of customs procedure, -</li> <li>- application of measures related to prohibitions and restrictions, commercial policy,</li> <li>- introduction of goods to the customs territory of the Community etc.</li> </ul> <p>Non compliant behaviour in the past increases the chance that future rules and regulations will be</p>	<ul style="list-style-type: none"> <li>- active compliance policy by the operator;</li> <li>- written operating instructions are preferred as regards responsibilities for carrying out checks on accuracy, completeness and timelines of transactions and disclose irregularities/errors, including suspicion of criminal activity to customs authorities;</li> <li>- procedures to investigate and report errors found and to review and improve processes;</li> <li>- the competent/responsible person within the business should be clearly identified and arrangements for cases of holidays or other types of absences should be installed;</li> <li>- implementation of internal compliance measures; use of audit resources to test/assure procedures are correctly applied;</li> <li>- internal instructions and training programmes to ensure staff are aware of customs requirements.</li> </ul>	SAQ - 2.1

	ignored/violated. Insufficient awareness of breaches against customs requirements.		
--	---	--	--

## 2. The applicants accounting and logistical system (Section 3 from SAQ)

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

### 2.1. Accounting system (Subsection 3.2 from SAQ)

Indicator	Risk description	Possible solutions	References
Computerised environment	The risk that an accounting system is inconsistent with the generally accepted accounting principles applied in the Member State. Incorrect and/or incomplete recording of transactions in the accounting system.	- segregation of duties between functions should be examined in close correlation with the size of the applicant. For example, a micro-enterprise which is performing road transport business with a small amount of everyday operations: packing, handling, loading/unloading of goods might be assigned to the driver of the truck. The receipt of the goods, their entering in the administration system and the payment/receipt of invoices should be assigned however to another person(s);	SAQ - 3.2 ISO 9001:2001, section 6.3
Integrated accounting system	Lack of reconciliation between stock and accounting records. Lack of segregation of duties between functions. Lack of physical or electronic access to customs and, where appropriate, transport records; Breaching the audit-ability. Inability to readily undertake an audit due to the way in which the applicant's accounting system is structured Complex management system offers possibilities to cover-up illegal	- implement a warning system which identify suspicious transactions;  - develop interface between customs clearance and accounting software to avoid typing errors; - implement an enterprise resource planning (ERP); - develop training and prepare instructions for the use of the software.	

	transactions.		
--	---------------	--	--

## 2.2. Audit trail (Subsection 3.1 from SAQ)

Indicator	Risk description	Possible solutions	References
Audit trail	The absence of an adequate audit trail mitigates against an efficient and effective audit based customs control.  Lack of control over the system's security and access.	- consultation with the customs authorities prior to the introduction of new customs accounting systems to ensure they are compatible with customs requirements; - testing and assuring the existence of the audit trail during the pre audit phase.	SAQ 3.1 ISO 9001:2001, section 6.3

## 2.3. Logistic system that distinguishes community and non community goods

Indicator	Risk description	Possible solutions	References
Mix community and non community goods	Lack of logistical system which distinguishes between Community and non-Community goods. Substitution of non community goods	- internal control procedures - data entry integrity checks	

## 2.4. Internal control system (Subsection 3.3 from SAQ)

Indicator	Risk description	Possible solutions	References
Internal control procedures	Inadequate control within the applicant over the business processes.  No/weak internal control procedures offer possibilities for fraud, unauthorised or illegal activities.  Incorrect and/or incomplete recording of transactions in the accounting	- appointment of a responsible person for quality in charge of procedures and internal controls of the company; - make each head of department fully aware of internal controls of their own department; - record the dates of internal controls or audits and correct identified weakness through corrective actions; -notify the customs authorities if fraud, unauthorised or illegal activities are discovered; - make the relevant internal control procedures available to the personnel concerned; - create a folder/a file in which each type of goods is linked with its own related customs	SAQ 3.3 ISO 9001:2001, , sections 5.5, 6.3, 7.4, 7.5, 8.2, 8.5

	system. Incorrect and or incomplete information in customs declarations and other statements to customs.	information (tariff code, customs duty rates, origin and customs procedure); - appointment of responsible person(s) for managing and updating the customs regulations applicable (inventory of regulations): i.e. update data in the enterprise resource planning (ERP), clearance or accounting, software.	
--	---	--	--

## 2.5. Flow of goods (Subsection 3.4 from SAQ)

Indicator	Risk description	Possible solutions	References
General	Lack of control over stock movements offers possibilities to add dangerous and/or terrorist related goods to the stock and to take goods out of stock without appropriate registration.	- records of stock movements; - regular stock reconciliations; - arrangements for investigating stock discrepancies; - being able to distinguish in the computer system whether goods are cleared or are still subject to duties and taxes.	SAQ - 3.4 ISO 9001:2001, section 6.3
Incoming flow of goods	Lack of reconciliation between goods ordered, goods received and entries into accounting records.	- records of incoming goods; - reconciliation between purchase orders and goods received; - arrangements for returning/rejecting goods, for accounting and reporting short and over shipments and for identifying and amending incorrect entries in the stock record; - formalisation of procedures for import; - perform regular inventories; - perform punctual consistency check of input / output of goods; - secure storage areas 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 fight against the substitution of goods.	SAQ - 3.4 ISO 9001:2001, section 6.3
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.	SAQ - 3.4 ISO 9001:2001, section 6.3
Outgoing flow of goods Delivery from warehouse and shipment and	Lack of reconciliation between stock records and entries to the accounting records.	- persons are appointed to authorise/oversee the sale/release process; - formalisation of procedures for export; - checks prior to release to compare the release order with the goods to be loaded; - arrangements for dealing with irregularities, short shipments and variations; - standard procedures for dealing with returned goods – inspection and recording;	SAQ - 3.4 ISO 9001:2001, sections 6.3, 7.1

transfer of goods		- check the discharge of declaration in case of with custom procedures with economic impact.	
-------------------	--	--	--

## 2.6. Customs routines (Subsection 3.5 from SAQ)

Indicator	Risk description	Possible solutions	References
General	<p>Ineligible use of the routines. Incomplete and incorrect customs declarations and incomplete and incorrect information about other customs related activities.</p> <p>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.</p> <p>Lack of routines for informing customs authorities about identified irregularities in compliance with customs requirements.</p>	<p>- implement formal procedures to manage/follow each customs activity and formalise specific clients (classification of goods, origin, value, etc.). These procedures are intended to ensure the continuity of customs department in case of the absence of assigned staff;</p> <p>- use Binding Tariff Information (BTI) that set the duties and import taxes and applicable regulations (sanitary, technical, trade policy measures, etc.);</p> <p>- use BOI which provides the administration's advice on :</p> <ul style="list-style-type: none"> <li>• the origin of the product you want to import or export, especially when the various stages of production have taken place in different countries;</li> <li>• whether or not to receive preferential treatment under a convention or international agreement;</li> </ul> <p>- setting up formal procedures for the determination and the declaration of customs value (valuation method, calculation, boxes of the declaration to fulfil and documents to produce);</p> <p>- implement procedures for notification of any irregularities to customs authorities.</p>	SAQ - 3.5 ISO 9001:2001, section 6.2.2
Representation through third parties	Lack of control	<p>- routines to check third parties work (e. g. on customs declarations) and identifying irregularities or violations be representatives should be implemented. It is not sufficient to rely completely on outsourced services;</p> <p>- verification of the competence of the representative used;</p> <p>- if the responsibility for completing customs declarations is outsourced:</p> <ul style="list-style-type: none"> <li>• specific contractual provisions to control customs data</li> <li>• a specific procedure to transmit the data which are necessary for the declarant to determine the tariff (i.e. technical specifications of goods, samples, etc.)</li> </ul> <p>- if externalisation of the management of customs, the outsourcing can be committed to a declarant who has obtained the status of approved exporter (guarantee of good command of origin rules);</p> <p>- implement formal procedures of internal control in order to verify the accuracy of customs data used.</p>	

Licences for import and/or export connected to commercial policy measures or to trade in agricultural goods	Ineligible use of goods	<ul style="list-style-type: none"> <li>- standard procedures to record licences;</li> <li>- regular internal controls of the licences validity and registration;</li> <li>- segregation of duties between registration and internal controls;</li> <li>- standards for reporting irregularities;</li> <li>- procedures to ensure the use of goods are consistent with the licence.</li> </ul>	
---	-------------------------	---	--

## 2.7. Procedures as regards back-up, recovery and fall-back and archival options (Subsection 3.6 from SAQ)

Indicator	Risk description	Possible solutions	References
Requirements for record keeping /archiving	<p>Inability to readily undertake an audit due to the loss of information or bad archiving.</p> <p>Lack of back-up routines.</p> <p>Lack of satisfactory procedures for the archiving of the applicant's records and information.</p> <p>Deliberate destruction or loss of relevant information</p>	<ul style="list-style-type: none"> <li>- the presentation of an ISO 27001 certificate demonstrates high standards in IT security;</li> <li>- procedures for back-up, recovery and data protection against damage or loss;</li> <li>- contingency plans to cover systems disruption/failure;</li> <li>- procedures for testing back-up and recovery;</li> <li>- save the customs archives and commercial documents in secure premises;</li> <li>- have a classification scheme;</li> <li>- adhere to archive legal deadlines.</li> </ul>	<p>ISO 9001:2001, section 6.3</p> <p>ISO 17799:2005</p> <p>ISO 27001:2005</p> <p>ISO norms for standards in the IT security</p>

## 2.8 Information security – protection of computer systems (Subsection 3.7 from SAQ)

Indicator	Risk description	Possible solutions	References
General	Unauthorised access and/or intrusion to the economic operator's computer systems and or programs.	<ul style="list-style-type: none"> <li>- IT security policy, procedures and standards should be in place and available to staff;</li> <li>- the presentation of an ISO 27001 certificate demonstrates high standards in IT security;</li> <li>- information security policy;</li> <li>- information security officer;</li> <li>- information security assessment or identifying issues relating to IT risk;</li> <li>- procedures for granting/withdrawing access rights to authorised persons;</li> <li>- using encryption software where appropriate;</li> <li>- firewalls;</li> <li>- anti-virus protection;</li> </ul>	<p>SAQ - 3.7</p> <p>ISO 17799:2005</p> <p>ISO 27001:2005</p>

		<ul style="list-style-type: none"> <li>- password protection;</li> <li>- testing against unauthorised access;</li> <li>- limit access to server rooms to authorised persons;</li> <li>- perform tests intrusion at regular intervals;</li> <li>- implement procedures for dealing with incidents.</li> </ul>	
General	Deliberate destruction or loss of relevant information.	<ul style="list-style-type: none"> <li>- contingency plan for loss of data;</li> <li>- back-up routines for system disruption/failure;</li> <li>- procedures for removing access rights.</li> </ul>	ISO/PAS 28001:2006, section A 3.3 ISO 27001:2005

## 2.9 Information security – documentation security (Subsection 3.8 from SAQ)

Indicator	Risk description	Possible solutions	References
General	<p>Misuse of the economic operator's information system to endanger the supply chain.</p> <p>Deliberate destruction or loss of relevant information.</p>	<ul style="list-style-type: none"> <li>- the presentation of an ISO 27001 certificate demonstrates high standards in IT security;</li> <li>- procedures for authorised access to documents;</li> <li>- filing and secure storage of documents;</li> <li>- procedures for dealing with incidents and taking remedial action;</li> <li>- recording and back-up of documents, including scanning;</li> <li>- contingency plan to deal with losses;</li> <li>- possibility to use encryption software if needed;</li> <li>- commercial agents to be aware of security measures while travelling (never consult sensitive documents in transport);</li> <li>- set up access levels to strategic information according to different categories of personnel;</li> <li>- handle discarded computers in a secure manner;</li> <li>- arrangements with business partners for protecting/use of documentation.</li> </ul>	SAQ - 3.8 ISO/PAS 28001:2006, section A 4.2 ISO 17799:2005 ISO 27001:2005
Security and safety requirements imposed on others	<p>Misuse of the economic operator's information system to endanger the supply chain.</p> <p>Deliberate destruction or loss of relevant information.</p>	<ul style="list-style-type: none"> <li>- requirements to protect data included in contracts;</li> <li>- procedures to control and audit the requirements in contracts.</li> </ul>	

### 3. Financial solvency (Section 4 from SAQ)

Criterion: Proven financial solvency (Article 14j of the CCIP)

#### 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.	<ul style="list-style-type: none"> <li>- examine the balance 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;</li> <li>- internal monitoring procedures to prevent financial threats.</li> </ul>	

### 4. Security and safety requirements (Section 5 from SAQ)

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

#### 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	<ul style="list-style-type: none"> <li>- risk and threat self-assessment is carried out, regularly reviewed/updated and documented;</li> <li>- identify precisely security and safety risks arising from activities of the company;</li> <li>- assess the risks related to security and safety (% of probability or risk level: low/medium/high);</li> <li>- make sure all the relevant risks are covered by preventive and or corrective measures.</li> </ul>	SAQ - 5.1.1 ISO/PAS 28001:2006, section A.4.2 ISPS Code
Internal organisation	Inadequate coordination about security and safety within the applicant's company.	<ul style="list-style-type: none"> <li>- appointment of responsible person with sufficient authority to coordinate and implement appropriate security measures in all relevant departments of the company;</li> <li>- implement formal procedures to manage/follow each logistical activity from a security and safety point view;</li> <li>- implement procedures to ensure security and safety of goods in cases of holidays or other types of absences of assigned staff.</li> </ul>	SAQ - 5.1.3 ISO/PAS 28001:2006, section A.3.3 ISO 9001:2001, section 5.5.1 ISPS Code

Internal control procedures	Inadequate control within the applicant's company over security and safety issues	<ul style="list-style-type: none"> <li>- implement internal control procedures on security &amp; safety procedures/issues;</li> <li>- procedures for recording and investigating security incidents, including reviewing the risk and threat assessment and taking remedial action where appropriate.</li> </ul>	SAQ - 5.1.6 ISO/PAS 28001:2006, section A.3.3, A.4.2 ISPS Code
Internal control procedures	Inadequate control within the applicant's company over security and safety issues	<ul style="list-style-type: none"> <li>- registration can be done in a file containing for example date, observed anomaly, name of the person who has detected the anomaly, countermeasure, signature of the responsible person;</li> <li>- make the register of security and safety incidents available to employees of the company.</li> </ul>	ISO/PAS 28001:2006, section A.3.3, A.4.2 ISPS Code
Security and safety requirements specific to goods	Tampering of goods	<ul style="list-style-type: none"> <li>- implement a goods tracking system;</li> <li>- special packaging or storage requirements for hazardous goods.</li> </ul>	ISPS Code

#### 4.2. Entry and access to premises (Subsection 5.2 from SAQ)

Indicator	Risk description	Possible solutions	References
Routines for access or entry of vehicles, persons and goods	Unauthorised access or entry of vehicles, persons or goods to the premises and/or close to the loading and shipping area.	<ul style="list-style-type: none"> <li>- the number of vehicles with access to the premises should be as limited as possible;</li> <li>- for that reason parking for staff should be preferably outside the security ring;</li> <li>- in addition it can be implemented, if possible, that trucks are waiting before and after loading in a separate area outside the security area. Only signed in trucks will get access to the loading area on demand for the time of the loading;</li> <li>- the usage of badges is reasonable. The badges should have a photo on it. If there is no photo on it the badges should at least indicate the name of the operator or the premises they are valid for (risk for misuse in case they are lost). The use of badges needs to be supervised by a responsible person. Visitors should have temporary identification badges and be accompanied at all time. Data on all entries including names of visitors/drivers, arrival/departure time and attendant should be recorded and stored in appropriate form (e.g. logbook, IT system). Badges not to be used twice in a row to avoid passing the badge to a companion;</li> <li>- access control with codes: routines for changing the code regularly;</li> <li>- badges and codes should only be valid during the working hours of the employee.</li> </ul>	SAQ - 5.2 ISO/PAS 28001:2006, section A.3.3 ISPS Code
Standard operating procedures in	No proper action if intrusion has been discovered.	<ul style="list-style-type: none"> <li>- implement procedures for cases of intrusion or unauthorised entry;</li> <li>- conduct intrusion tests and record the test results and, if necessary, implement corrective actions;</li> </ul>	ISO/PAS 28001:2006, section A.3.3 ISPS Code

case of intrusion	- use of incident report or other appropriate form to record incidents and action taken; - implement remedial measures as a result of incidents related to unauthorised entry.
-------------------	---

#### 4.3. Physical security (Subsection 5.3 form SAQ)

Indicator	Risk description	Possible solutions	References
External boundaries of premises	Inadequate protection of the premises against external intrusion.	- where appropriate secure perimeter fencing is in place with regular inspections to check integrity and damage and planned maintenance and repairs; - where appropriate controlled areas for authorised personnel only are adequately signed and controlled.	SAQ - 5.3 ISO/PAS 28001:2006, section A.3.3 ISPS Code
Gates and gateways	Existence of gates or gateways which are not monitored.	- all gates or gateways should be secured by using of appropriate measures, i.e CCTV and/or entry control system (lightening, beamers, etc.); - if appropriate, implement procedures to ensure the protection of access points.	ISO/PAS 28001:2006, section A.3.3 ISPS Code
Locking devices	Inadequate locking devices for external and internal doors, windows, gates and fences.	- instruction/procedure on use of keys is in place and available for staff concerned; - only authorised personnel have access to keys for locked buildings, sites, rooms, secure areas, filing cabinets, safes, vehicles and machinery; - conducting periodic inventories of locks and keys; - log attempts of unauthorised access and check this information on a regular basis.	SAQ - 5.3.4 ISO/PAS 28001:2006, section A.3.3
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.	SAQ - 5.3.3
Procedures for access to keys	Lack of adequate procedures for access to keys. Unauthorised access to keys.	- a key access control procedure should be implemented; - keys should be handed out only after registration and be given back immediately after usage. The return of the key has to be registered, too.	ISO/PAS 28001:2006, section A.3.3
Internal physical security measures	Inappropriate access to internal sections of the premises.	- implement a process to distinguish the different categories of employees in the premises (i.e. jackets, badges); - access controlled and personalised according to employees' position.	ISO/PAS 28001:2006, section A.3.3, A.4.2 ISPS Code
Parking of private vehicles	Lack of adequate procedures for parking of private vehicles. Inadequate protection of the premises against external intrusion.	- the number of vehicles with access to the premises should be as limited as possible; - specially designated car park areas for visitors and staff are remote from any cargo handling or storage areas; - identification of risks and threats of unauthorised entry of private vehicles to protected areas; - defined rules/procedure for entry of private vehicles in the applicant's premises.	

Maintenance external boundaries and buildings	Inadequate protection of the premises against external intrusion as a result of inappropriate maintenance.	- regular maintenance of the external boundaries of the premises and the buildings each time an anomaly is detected.	ISO/PAS 28001:2006, section A.3.3
---	--	--	-----------------------------------

#### 4.4. Cargo units (Subsection 5.4 from SAQ)

Indicator	Risk description	Possible solutions	References
Routines for access to cargo units	Lack of adequate procedures for access to cargo units. Unauthorised access to cargo units.	<ul style="list-style-type: none"> <li>- identification of risks and threats of unauthorized access to shipping areas, loading docks and cargo areas;</li> <li>- implement procedures governing access to shipping areas, loading docks and cargo areas;</li> <li>- cargo units are placed in a secure area or other measures are taken to assure the integrity of the cargo unit;</li> <li>- access to the area where cargo units are held is restricted to authorised persons;</li> <li>- share planning between the transport department and the goods reception desk.</li> </ul>	SAQ - 5.4.1 ISO/PAS 28001:2006, section A.3.3 ISPS Code
Routines for ensuring the integrity of cargo units	Tampering with cargo units.	<ul style="list-style-type: none"> <li>- procedures for monitoring &amp; checking the integrity of cargo units;</li> <li>- procedures for recording, investigating and taking remedial action when unauthorised access or tampering has been discovered;</li> <li>- where appropriate supervision by CCTV.</li> </ul>	SAQ -5.4.2 ISO/PAS 28001:2006, section A.3.3 ISPS Code
Use of seals	Tampering with cargo units.	<ul style="list-style-type: none"> <li>- use of container seals that are compliant with ISO/PAS 17712 or other appropriate type of system ensuring the integrity of cargo during transportation;</li> <li>- seals stored in a secure location;</li> <li>- register of seals is maintained (including used ones);</li> <li>- regular reconciliation between register and seals held;</li> <li>- where applicable make arrangements with business partners to check the seals (integrity and numbers) at arrival.</li> </ul>	SAQ - 5.4.3 ISO/PAS 17712
Procedures for inspecting the structure of the cargo unit including ownership of cargo units	Use of hidden places in cargo units for smuggling purposes.  To have incomplete control of the cargo units.	<ul style="list-style-type: none"> <li>- procedures to examine the integrity of the cargo unit prior to loading;</li> <li>- where appropriate use of seven point inspection process (front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage prior to loading);</li> <li>- other kinds of inspections depending on the kind of cargo unit.</li> </ul>	SAQ - 5.4.4; SAQ - 5.4.5 ISO/PAS 28001:2006, section A.3.3
Maintenance of cargo units	Tampering with cargo units.	<ul style="list-style-type: none"> <li>- regular programme of routine maintenance;</li> <li>- if maintenance is carried out by a third party, procedures to examine the integrity of the cargo unit after that.</li> </ul>	SAQ - 5.4.5 ISO/PAS 28001:2006, section A.3.3

Standard operating procedures in case of intrusion and/or tampering with cargo units	No proper action if unauthorised access or tampering has been discovered.	- appropriate procedures laid down on what measures should be taken when an unauthorised access or tampering is discovered.	ISO/PAS 28001:2006, section A.3.3
--	---	---	-----------------------------------

#### 4.5 Logistical processes (Subsection 5.5 from SAQ)

Indicator	Risk description	Possible solutions	References
Active means of transport entering/leaving the customs territory of the Community	Lack of control over the transport of goods.	<ul style="list-style-type: none"> <li>- use of track and trace technology can show unusual stops or delays which could have affected the security of the goods;</li> <li>- special procedures for the selection of carriers/freight forwarders;</li> <li>- make arrangements with business partners to check the seals (integrity and numbers) when the goods arrive at their premises.</li> </ul>	SAQ - 5.5

#### 4.6 Non-fiscal requirements (Subsection 5.6 from SAQ)

Indicator	Risk description	Possible solutions	References
Non-fiscal aspects	Ineligible use of goods falling under prohibitions and restrictions or commercial policy measures.	<ul style="list-style-type: none"> <li>- procedures for handling of goods with non-fiscal aspects;</li> <li>- appropriate routines and procedures should be established: <ul style="list-style-type: none"> <li>-- to distinguish goods subject to non-fiscal requirements and other goods;</li> <li>-- to check if the operations are carried out in accordance with current (non-fiscal) legislation;</li> <li>-- to handle goods subject to restrictions/prohibitions/embargo and dual-use goods;</li> <li>-- to handle licenses as per the individual requirements.</li> </ul> </li> <li>- awareness training/education for staff dealing with goods with non-fiscal aspects.</li> </ul>	SAQ - 5.6

#### 4.7 Incoming goods (Subsection 5.7 from SAQ)

Indicator	Risk description	Possible solutions	References
-----------	------------------	--------------------	------------

Routines for checking incoming transport	Introduction, exchange or loss of received goods.  Uncontrolled incoming goods which may pose a security or safety risk.	<ul style="list-style-type: none"> <li>- maintain a schedule of expected arrivals;</li> <li>- procedures for handling unexpected arrivals;</li> <li>- perform consistency checks between incoming goods and entries in the logistics systems;</li> <li>- procedures for testing the integrity of the means of transport.</li> </ul>	SAQ - 5.7.1 ISO 9001:2001, section 6.2.2 ISO/PAS 28001:2006, section A.3.3
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.	<ul style="list-style-type: none"> <li>- procedures for ensuring staff are aware of security requirements;</li> <li>- management/supervision checks to ensure the security requirements are complied with.</li> </ul>	SAQ - 5.7.2 ISO/PAS 28001:2006, section A.3.3
Supervision for the receipt of goods	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	<ul style="list-style-type: none"> <li>- personnel assigned to receive the driver on arrival and supervise the unloading of goods;</li> <li>- use pre-arrival information;</li> <li>- procedures to ensure assigned staff are present at all times and goods are not left unsupervised</li> <li>- perform consistency checks between incoming goods and the transport documents.</li> </ul>	SAQ - 5.7.3 ISO/PAS 28001:2006, section A.3.3
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	<ul style="list-style-type: none"> <li>- procedures for checking the integrity of seals and the correspondence of the seal number with the number in the documents;</li> <li>- appointment of designated authorised person.</li> </ul>	SAQ - 5.7.3 ISO/PAS 28001:2006, section A.3.3 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	<ul style="list-style-type: none"> <li>- checks to compare the goods with the accompanying transport and customs documents, picking lists and purchase orders;</li> <li>- checks on completeness by weighing, counting, and tallying and checks on the uniform marking of goods;</li> <li>- updating stock records as soon as possible on arrival;</li> <li>- place goods that pose an anomaly in a specific and secure area and create a process to manage these goods.</li> </ul>	SAQ - 5.7.4, 5.7.5, 5.7.6 ISO 9001:2000, section. 7.4
Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	- procedures to record and investigate irregularities e.g. short shipments, broken anti-tampering devices including reviewing procedures and taking remedial action.	SAQ - 5.7.7

#### 4.8 Storage of goods (Subsection 5.8 from SAQ)

Indicator	Risk description	Possible solutions	References
-----------	------------------	--------------------	------------

Assignment of storage location	Inadequate protection of the storage area against external intrusion	- procedures governing access to the area for storage of goods; - an area or areas is/are designated for the storage of goods with CCTV surveillance system or other appropriate controls.	SAQ - 5.8.1 & 5.8.2
Goods to be stored outdoors	Manipulation of those goods	- need to use adequate lighting and if appropriate CCTV surveillance; - integrity of those goods has to be checked and documented before loading; - if possible show the destination of those goods at the latest possible stage (for i.e. bar codes instead of plain text indicating destination ).	
Internal control procedures	Lack of procedures to ensure security and safety of stored goods. No proper action if discrepancies and/or irregularities are discovered.	- procedures for regular stocktaking and recording and investigating any irregularities/discrepancies including reviewing procedures and taking remedial action.	SAQ - 5.8.3 ISO 9001:2001, section 2.2
Separate storage of different goods	Unauthorised substitution of goods and/or tampering with goods.	- location of goods is recorded in stock records; - where appropriate different goods e. g community/non community goods, hazardous goods, high value goods, overseas/domestic goods are stored separately.	SAQ - 5.8.4 TAPA (Technology Asset Protection Association) Certificate
Additional security and safety measures for access to goods	Unauthorised access to the goods.	- authorised access to the storage area only for designated staff; - visitors and third parties should have temporary identification badges and be accompanied at all time; - data on all visits including names of visitors/third parties, arrival/departure time and attendant should be recorded and stored in appropriate form (e.g. logbook, IT system); - if own storage area at another operator premises this area should be secured by regular communication between the operators involved and by visits and controls on spot by the AEO.	SAQ - 5.8.5 ISO/PAS 28001:2006, section A.3.3 ISPS Code

#### 4.9 Production of goods (Subsection 5.9 from SAQ)

Indicator	Risk description	Possible solutions	References
Assignment of production location Additional security and safety measures for access to goods	Lack of procedures to ensure security and safety of manufactured goods. Unauthorised access to the goods.	- an area is designated for production of goods with appropriate access controls; - authorised access to the production area only for designated staff; - visitors and third parties have to wear high visibility vests and be accompanied at all times; - procedures to ensure safety and security of production processes;	SAQ - 5.9.2 ISO/PAS 28001:2006, section A.3.3
Internal control	Lack of procedures to ensure security	- security processes and procedures should be established to assure the integrity of the production process, e.g. authorised access only for designated staff or appropriately authorised	ISO/PAS 28001:2006, section A.3.3

procedures	and safety of manufactured goods. Tampering with the goods.	persons, supervision and monitoring of the production process by systems and/or personnel.	
Packing of products	Incomplete control over the packing of the products. Introduction, exchange or loss of produced goods.	- wherever possible products should be packed in a way that tampering is easily to be detected. An example could be the use of special tape with brand names on it. The tape has to be kept under supervision in that case. Another solution is to use tape which cannot be removed residue-free; - technological aids to packing integrity may also be used e.g. CCTV surveillance, or weight checking; - if possible show the destination of those goods at the latest possible stage (for i.e. bar codes instead of plain text indicating destination ).	SAQ - 5.9.3
Quality inspection	Incomplete control over the flow of goods. Introduction, exchange or loss of produced goods.	- carry out random security and safety checks of produced goods at each stage of production.	

#### 4.10 Loading of goods (Subsection 5.10 from SAQ)

Indicator	Risk description	Possible solutions	References
Routines for checking outgoing transport	Lack of control of delivery of goods which might pose a security or safety risk.	- control the goods loaded (consistency checking / counting / weighing / load order of sales against the information from logistics departments). Check with the logistical system - procedures on reception of means of transport are in place; - strict access control to the loading area.	SAQ - 5.10.1 ISO/PAS 28001:2006, section A.3.3
Routines for verifying security measures imposed by others	Breach of agreed security arrangements with the risk of delivery of unsafe or insecure goods; delivery of goods which is not registered in a logistical system and of which you don't have any control.	- procedures for ensuring staff are aware of customer's security requirements; - management/supervision checks to ensure the security requirements are complied with.	SAQ - 5.10.3 ISO/PAS 28001:2006, section A.3.3
Supervision over loading of goods	Lack of supervision of loading of goods which might pose a security or safety risk.	- checks on completeness by weighing, counting, tallying and uniform marking of goods; - procedures for announcing drivers before arrival; - personnel assigned to receive the driver and supervise the loading of goods; - drivers have no unsupervised access to the loading area; - procedures to ensure assigned staff are present at all times and goods are not left unsupervised; - appointment of responsible person(s) to carry out checks on routines.	SAQ - 5.10.4 ISO/PAS 28001:2006, section A.3.3

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.	<ul style="list-style-type: none"> <li>- procedures for controlling, applying, checking and recording seals;</li> <li>- appointment of designated authorised person;</li> <li>- use of container seals that are compliant with ISO/PAS 17712.</li> </ul>	SAQ - 5.10.2 ISO/PAS 28001:2006, section A.3.3 ISO/PAS 11712:116 ISO PAS 17712
Administrative processes of the loading of goods	Delivery of goods which is not registered in a logistical system and of which you don't have any control and thus posing a security or safety risk.	<ul style="list-style-type: none"> <li>- checks to compare the goods with the accompanying transport and customs documents, loading/packing lists and sales orders;</li> <li>- updating stock records as soon as possible after departure.</li> </ul>	SAQ - 5.10.5 and 5.10.6
Internal control procedures	No proper action if discrepancies and/or irregularities are discovered.	- procedures to record and investigate irregularities e.g. short shipments, broken anti-tampering devices, customer returns, review procedures and take remedial action.	SAQ - 5.10.7 ISO/PAS 28001:2006, section A.3.3

#### 4.11 Security requirements on business partners (Subsection 5.11 from SAQ)

Indicator	Risk description	Possible solutions	Reference
Identification of business partners	Lack of mechanism for clear identification of the business partners.	<ul style="list-style-type: none"> <li>- procedure in place for identifying regular business partners and unknown clients/customers;</li> <li>- procedures to select and manage business partners where the transport is carried out by a third party;</li> <li>- implement a procedure to select subcontractors based on a list of regular and irregular subcontractors;</li> <li>- subcontractors can be selected on the basis of selection criteria or even of a company specific certification (which can be set up on the base of a certification questionnaire).</li> </ul>	
Security requirements imposed on others	Breach of agreed security arrangements with the risk of receiving or delivering unsafe or unsecured goods.	<ul style="list-style-type: none"> <li>- background checks used to select regular business partners e.g. through the use of internet or rating agencies;</li> <li>- security requirements (e.g. that all goods must be marked, sealed, packed, labelled in a certain way, subject to X-ray checks) are written into contracts with regular business partners;</li> <li>- requirement that contracts will not be further sub-contracted to unknown third parties;</li> <li>- conclusions provided by experts/external auditors, not related to regular business partners, on complying with security requirements;</li> <li>- evidence that business partners hold relevant accreditations/certificates to prove they comply with international security standards;</li> <li>- procedures for carrying out additional security checks on transactions with unknown or</li> </ul>	SAQ - 5.11 ISO/PAS 28001:2006, section A.3.3

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

#### 4.12 Personnel security (Subsection 5.12 from SAQ)

Indicator	Risk description	Possible solutions	References
Employment policy including for temporary personnel	Infiltration of staff that could pose a security risk.	<ul style="list-style-type: none"> <li>- background checks on prospective employees, e.g. previous employment history and references;</li> <li>- additional checks on new or existing employees moving to security sensitive posts e.g. police checks on unspent convictions;</li> <li>- requirements on staff to disclose other employment, police cautions/bail, pending court proceedings, or convictions;</li> <li>- periodic background checks/reinvestigations for current personnel;</li> <li>- removal of computer access, return of security pass, keys and/or badge when staff leave or are dismissed;</li> <li>- checks on temporary staff applied at the same standard as permanent staff;</li> <li>- contracts with employment agencies detail level of security checks required;</li> <li>- procedures to ensure employment agencies comply with those standards.</li> </ul>	SAQ - 5.12.2; SAQ - 5.12.4  ISO/PAS 28001:2006, section A.3.3
Level of safety and security awareness of personnel	Lack of proper knowledge on security procedures related to different process (incoming goods, loading, unloading, etc.) with the consequence of accepting/loading/unloading unsafe or insecure goods.	<ul style="list-style-type: none"> <li>- staff awareness on security measures/arrangements related to different process (incoming goods, loading, unloading, etc.);</li> <li>- set up a register for recording security and safety anomalies and discuss this with staff on a regular basis;</li> <li>- procedures in place for employees to identify and report suspicious incidents;</li> <li>- pamphlets on security and safety issues can be displayed in specific areas and communicated via a notice-board;</li> <li>- display the security &amp; safety rules in the relevant areas (loading/unloading etc.). The signs must be visible internally (in the sites) and externally (places dedicated to the drivers, temporaries, various partners).</li> </ul>	ISO/PAS 28001:2006, section A.3.3
Security and Safety training	Lack of mechanisms for training employees on safety and security requirements and, consequently, inadequate awareness of security requirements.	<ul style="list-style-type: none"> <li>- persons responsible for identifying training needs, ensuring delivery and keeping training records;</li> <li>- training employees to recognise potential internal threats to security, detection of intrusion/tampering and preventing unauthorised access to secure premises, goods, vehicles, automated systems, seals and records;</li> <li>- conducting tests with “unsafe” goods or occasions;</li> <li>- security and safety training can be part of industrial safety training to outreach all staff.</li> </ul>	SAQ - 5.12.3  ISO/PAS 28001:2006, section A.3.3

### 4.13 External services (Subsection 5.13 from SAQ)

Indicator	Risk description	Possible solutions	References
External services used for various areas, i.e. packing of products, security, etc.,	<p>Infiltration of staff that could pose a security risk.</p> <p>Incomplete control over the flow of goods</p>	<ul style="list-style-type: none"> <li>- security requirements e.g. identity checks on employees, restricted access controls are written into contractual agreements;</li> <li>- monitoring compliance with these requirements;</li> <li>- use of different badges for external staff;</li> <li>- restricted or controlled access to computer systems;</li> <li>- supervise external services where appropriate;</li> <li>- establish security arrangements and or auditing procedures to ensure the integrity of the goods.</li> </ul>	<p>SAQ 5.13 ISO/PAS 28001:2006, section A.3.3</p>