PART 5

Annex 2

Threats, Risks and Possible solutions

This document provides a list of the most significant **risks related to the AEO authorisation** and monitoring process, and at the same time, it provides a list of possible solutions on how to keep these risks under control. Possible solutions proposed for one indicator can be applicable to more than one risk area identified. The suggested list is neither exhaustive nor definitive and possible solutions will in practice vary from case to case. They will be influenced by and have to be proportional to the size of the operator, type of goods, type of automated systems and level of modernization of the operator. The 'Threats, risks and possible solution' document **is addressed both to customs validators and economic operators to facilitate the audit** and examination to ensure compliance with AEO criteria

1. Compliance record

Criterion: An appropriate record of compliance with customs requirements (AI 38/2017 article 7)

Indicator	Risk description	Possible solutions	References
Compliance with customs requirements	Non-compliant behaviour with regard to: - fulfilment of customs declarations including	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,	PVV -2.1

	incorrect classification, valuation, origin, - use of customs procedures - taxation rules, - application of measures related to prohibitions and restrictions, commercial policies - introduction of goods to the customs territory Non-compliant behaviour in the past increases the chance that future rules and regulations will be ignored/violated. Insufficient awareness of breaches against customs requirements.	completeness and timelines of transactions and disclose irregularities/errors, including suspicion of criminal activity to customs authorities; procedures to investigate and report errors found and to review and improve processes; The competent/responsible person within the business should be clearly identified and arrangements for cases of holidays or other types of absences should be installed; implementation of internal compliance measures; use of audit resources to test/assure procedures are correctly applied; internal instructions and training programmes to ensure staff are aware of customs requirements.	

2. The applicants accounting and logistical system

Criterion: A satisfactory system of managing commercial and where appropriate, transport records, which allow appropriate customs controls (AI 38/2017 article 8)

2.1. Accounting system

Indicator	Risk description	Possible solutions	References
Computerised 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	- segregation of duties between functions should be examined in close correlation with the size of the applicant. For example, a micro-enterprise which is performing road transport business with a small amount of everyday operations: packing, handling, loading/unloading of goods might be assigned to the driver of the truck. The receipt of the goods, their entering in the administration system and the payment/receipt of invoices should be assigned however to another person(s); implement a warning system which identify suspicious transactions; - develop interface between customs clearance and accounting software to avoid typing errors; - implement an enterprise resource planning (ERP); develop training and prepare instructions for the use of the software; allow cross checks of information.	ISO 9001:2015, part 6.3 PVV-3.2

	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 transactions. No historical data available.		

2.2. Audit trial

Indicator	Risk description	Possible solutions	References
Audit trial	The absence of an adequate audit trail mitigates against an efficient and effective audit based customs control. Lack of control over the system's security and access.	- consultation with the customs authorities prior to the introduction of new customs accounting systems to ensure they are compatible with customs requirements; - testing and assuring the existence of the audit trail during the validation phase.	ISO 9001:2015, part 6.3 PVV-3.1

Indicator	Risk description	Possible solutions	References

Mix of Customs cleared and non-Customs cleared goods	Lack of logistical system which distinguishes between Customs cleared and non-Customs cleared goods. Substitution of Customs cleared and non-Customs cleared goods	Internal control procedures data entry Integrity checks to verify if the data entries are correct	

2.3 **Logistical system that distinguishes domestic and foreign goods**

2.3. Internal control system

Indicator	Risk description	Possible solutions	References
Internal control procedures	Inadequate control within the applicant over the business processes. No/weak internal control procedures offer possibilities for fraud, unauthorised or illegal activities. Incorrect and/or	- 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;	ISO 9001:2015, parts 5, 6, 7 and 8 PVV-3.3

	incomplete recording of transactions in the accounting system. Incorrect and or incomplete information in customs declarations and other statements to customs.	- record the dates of internal controls or audits and correct identified weakness through corrective actions; - notify the customs authorities if fraud, unauthorised or illegal activities are discovered; - make the relevant internal control procedures available to the personnel concerned; create a folder/a file in which each type of goods is linked with its own related customs information (tariff code, customs duty rates, origin and customs procedure) depending on the concerned volume of goods; - appointment of responsible person(s) for managing and updating the customs regulations applicable (inventory of regulations): i.e. update data in the enterprise recourse planning (ERP), clearance or accounting, software; - Inform and educate staff regarding inaccuracies and how one can prevent them from happening. Having procedures for recording and correcting errors and transactions in place	

2.4. Flow of goods

Indicator	Risk description	Possible solutions	References
General	Lack of control over stock movements offers possibilities to add dangerous and/or terrorist related goods to the stock and to take goods out of stock without appropriate registration.	- Information of relevant staff and submission of declaration as scheduled; - records of stock movements; - regular stock reconciliations; - arrangements for investigating stock discrepancies; being able to distinguish in the computer system whether goods are cleared or are still subject to duties and taxes.	ISO 9001:2015, part 6.3 PVV-3.4
Incoming flow of goods	Lack of reconciliation between goods ordered, goods received and entries into accounting records.	- records of incoming goods; reconciliation between purchase orders and goods received; - arrangements for returning/rejecting goods, for accounting and reporting short and over shipments and for identifying and amending incorrect entries in the stock record; - formalisation of procedures for import; - perform regular inventories; - perform punctual consistency check of input / output of goods; - secure storage areas (special shell protection, special access routines) to fight against the substitution of goods.	
Storage	Lack of control over stock movements.	- clear assignment of storage areas; - regular stock-taking procedures; - secure storage areas to protect against the substitution of goods.	ISO 9001:2015, part 6.3 PVV-3.4

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, part 6.3 PVV-3.4
Outgoing flow of goods Delivery from warehouse and shipment and transfer of goods	Lack of reconciliation between stock records and entries to the accounting records.	- persons are appointed to authorise/oversee the sale/release process; - formalisation of procedures for export; - checks prior to release to compare the release order with the goods to be loaded; - arrangements for dealing with irregularities, short shipments and variations; - standard procedures for dealing with returned goods – inspection and recording; - check the discharge of declaration in case of with custom procedures with economic impact.	ISO 9001:2015, parts 6.3 and 7.1 PVV-3.4

2.6 Customs routine

Indicator	Risk description	Possible solutions	References
General	Ineligible use of the routines. Incomplete and incorrect customs declarations and incomplete and incorrect	- 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	ISO 9001:2015, part 6.2.2 PVV-3.5

	information about other customs related activities. The use of incorrect or outdated standing data, such as article numbers and tariff codes: - Incorrect classification of the goods - incorrect tariff code -Incorrect customs value. Lack of routines for informing customs authorities about identified irregularities in compliance with customs requirements.	customs department in case of the absence of assigned staff; whether or not to receive preferential treatment under a convention or international agreement; setting up formal procedures for the determination and the declaration of customs value (valuation method, calculation, boxes of the declaration to fulfil and documents to produce); - implement procedures for notification of any irregularities to customs authorities.	
Representation through third parties	Lack of control	- routines to check third parties work (e. g. on customs declarations) and identifying irregularities or violations be representatives should be implemented. It is not sufficient to rely completely on outsourced services; - verification of the competence of the representative used; - if the responsibility for completing customs declarations is outsourced: specific contractual provisions to control customs data a specific	

		procedure to transmit the data which are necessary for the declarant to determine the tariff (i.e. technical specifications of goods, samples, etc.) if externalisation of the exportation of goods by an approved exporter, the outsourcing can be committed to a customs agent allowed to act as the authorised representative, as long as the agent is in a position to prove the originating status of the goods. implement formal procedures of internal control in order to verify the accuracy of customs data used.	
Licences for import and/or export connected to commercial policy measures or to trade in agricultural goods	Ineligible use of goods	- standard procedures to record licences; - regular internal controls of the licences validity and registration; - segregation of duties between registration and internal controls; - standards for reporting irregularities; - procedures to ensure the use of goods are consistent with the licence.	

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

Indicator	Risk description	Possible solutions	References
Requirements for record keeping /archiving	Inability to readily undertake an audit due to the loss of information or bad archiving.	- the presentation of an ISO 27001 certificate demonstrates high standards in IT security;	- ISO 9001:2015, part 6.3 - ISO 17799;2005

	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	- procedures for back-up, recovery and data protection against damage or loss; - contingency plans to cover systems disruption/failure; - procedures for testing back-up and recovery; - save the customs archives and commercial documents in secure premises; - have a classification scheme; - adhere to archive legal deadlines.	- ISO 27001;2005 - ISO norms for standards in the IT security

2.8. Information security – protection of computer systems

Indicator	Risk description	Possible solutions	References
General	Unauthorised access and/or intrusion to the economic operator's computer systems and or programs.	- IT security policy, procedures and standards should be in place and available to staff; the presentation of an ISO 27001 certificate demonstrates high standards in IT security; - information security policy; - information security officer; - information security assessment or identifying issues relating to IT risk; - procedures for granting access rights to authorised persons; access rights are to be withdrawn immediately on	ISO 27001:2013

		transfer of duty or termination of employment. -access to data on need to know basis. using encryption software where appropriate; firewalls; anti-virus protection; - password protection on all PC Stations and possibly on important programmes If employees leave their workplace the computer should always secured via keyword Password should be made out of at least eight characters being a mixture of two or more of upper and lower letters, numbers and other characters. The longer the password, the stronger it is. Usernames and passwords should never be shared. testing against unauthorised access; - limit access to server rooms to authorised persons; perform tests intrusion at regular intervals; intrusion tests are to be recorded. implement procedures for dealing with incidents.	

General	Deliberate destruction or loss of relevant information.	- contingency plan for loss of data; - back-up routines for system disruption/failure; - procedures for removing access right;	ISO 28001:2006, part A 3.3 ISO 27001:2005

2.9. Information security – documentation security

Indicator	Risk description	Possible solutions	References
General	Misuse of the economic operator's information system to endanger the supply chain. Deliberate destruction or loss of relevant information.	- the presentation of an ISO 27001 certificate demonstrates high standards in IT security; - procedures for authorised access to documents; filing and secure storage of documents; - procedures for dealing with incidents and taking remedial action; - recording and back-up of documents, including scanning; - contingency plan to deal with losses; possibility to use encryption software if needed; - commercial agents to be aware of security measures while travelling (never consult sensitive documents in transport);	ISO 28001:2006, part A 4.2 ISO 27001:2005 ISP1799;2005 PVV-3.8

		- set up access levels to strategic information according to different categories of personnel; - handle discarded computers in a secure manner; - arrangements with business partners for protecting/use of documentation.	
Security and safety requirements imposed on others	Misuse of the economic operator's information system to endanger the supply chain. Deliberate destruction or loss of relevant information.	- requirements to protect data included in contracts; - procedures to control and audit the requirements in contracts.	

3. Financial solvency

Criterion: Proven financial solvency (AI 38/2017 article 9)

3.1. Proven solvency

Indicator	Risk description	Possible solutions	References

Insolvency/fail ure 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 (AI 38/2017 article 10)

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 28001:2006, part A.4.2 ISPS Code PVV-5.1.1

Security management and internal organisation	Inadequate coordination about security and safety within the applicant's company.	- appointment of responsible person with sufficient authority to coordinate and implement appropriate security measures in all relevant departments of the company; - implement security policy including formal procedures to manage/follow each logistical activity from a security and safety point view; - implement procedures to ensure security and safety of goods in cases of holidays or other types of absences of assigned staff;	ISO 28001:2007, part A.3.3 ISO 9001:2015, part 5.5.1 ISPS Code PVV 5.1.3
Internal control procedures	Inadequate control within the applicant's company over security and safety issues	- implement internal control procedures on security & safety procedures/issues; - procedures for recording and investigating security incidents, including reviewing the risk and threat assessment and taking remedial action where appropriate.	ISO 28001:2006, part A.3.3, A.4.2 ISPS Code PVV-5.1.6
Internal control procedurës	Inadequate control within the applicant's company over security and safety issues	- registration can be done in a file containing for example date, observed anomaly, name of the person who has detected the anomaly, countermeasure, signature of the responsible person; - make the register of security and safety incidents available to employees of the company.	ISO 28001:2006, part A.3.3, A.4.2 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	Unauthorised 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 be preferably outside the security ring; - in addition it can be implemented, if possible, that trucks are waiting before and after loading in a separate area outside the security area. Only signed in trucks will get access to the loading area on demand for the time of the loading; - the usage of badges is reasonable. The badges should have a photo on it. - If there is no photo on it the badges should at least indicate the name of the operator or the premises they are valid for (risk for misuse in case they are lost). - The use of badges needs to be supervised by a responsible person.	ISO 28001:2007, pjesa A.3 Kodi ISPS

		- Visitors should have temporary identification badges and be accompanied at all time. - Data on all entries including names of visitors/drivers, arrival/departure time and attendant should be recorded and stored in appropriate form (e.g. logbook, IT system) and are enumerated. - Badges not to be used twice in a row to avoid passing the badge to a companion; - access control with codes: routines for changing the code regularly; - badges and codes should only be valid during the working hours of the employee; Standardised procedures for the return of all access authorisations; - Visitors should be met and supervised by the business to prevent any unauthorised activities; - Identification badges for visitors have to be worn visible; - Speak to unknown persons; Corporate clothing to recognise unknown persons; - In case of temporary work (i.e. Maintenance work) a list of authorised workers of the outsourced company.	

Standard operating procedures in case of intrusion	No proper action if intrusion has been discovered.	- implement procedures for cases of intrusion or unauthorised entry; - conduct intrusion tests and record the test results and, if necessary, implement corrective actions; - use of incident report or other appropriate form to record incidents and action taken; - implement remedial measures as a result of incidents related to unauthorised entry.	ISO 28001:2006, part A.3.3 ISPS Code

4.3. Physical security

Indicator	Risk description	Possible solutions	References
External boundaries of premises	Inadequate protection of the premises against external intrusion.	- where appropriate secure perimeter fencing is in place with regular inspections to check integrity and damage and planned maintenance and repairs; - where appropriate controlled areas for authorised personnel only are adequately signed and controlled; - Irregular patrols of the security staff.	ISO 28001:2006, part A.3.3 ISPS Code PVV-5.3
Gates and gateways	Existence of gates or gateways which are not monitored.	- all gates or gateways in use should be secured by using of appropriate measures, i.e. CCTV and/or entry control system (lightening, beamers, etc.);	ISO 28001:2006, part A.3.3 ISPS Code

		- CCTV is only useful when the recordings are evaluable and can lead to contemporary reactions if appropriate, implement procedures to ensure the protection of access points.	
Locking devices	Inadequate locking devices for external and internal doors, windows, gates and fences.	- instruction/procedure on use of keys is in place and available for staff concerned; - only authorised personnel have access to keys for locked buildings, sites, rooms, secure areas, filing cabinets, safes, vehicles, machinery and air cargo; - conducting periodic inventories of locks and keys; - log attempts of unauthorised access and check this information on a regular basis; - Windows and doors should be locked when nobody is working in the concerned room / office.	ISO 28001:2006, part A.3.3 PVV-5.3.4
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.	PVV-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 28001:2006, part A.3.3
Internal physical security measures	Inappropriate access to internal sections of the premises.	- implement a process to distinguish the different categories of employees in the premises (i.e. jackets, badges); - access controlled and personalised according to employees' position.	ISO 28001:2006, part 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; - in case of non-separate parking area for visitors and employees, cars of the visitors should have an identification	

Maintenance external boundaries and buildings	Inadequate protection of the premises against external intrusion as a result of inappropriate maintenance.	- regular maintenance of the external boundaries of the premises and the buildings each time an anomaly is detected.	ISO 28001:2007, part A.3

4.4. Cargo units

Indicator	Risk description	Possible solutions	References
Routines for access to cargo units	Lack of adequate procedures for access to cargo units. Unauthorised access to cargo units.	- identification of risks and threats of unauthorized access to shipping areas, loading docks and cargo areas; - implement procedures governing access to shipping areas, loading docks and cargo areas; cargo units are placed in a secure area (e.g. a fenced area, an area with video surveillance or monitored by security personnel) or other measures are taken to assure the integrity of the cargo unit; - access to the area where cargo units are held is restricted to authorised persons; - share planning between the transport department and the goods reception desk.	ISO 28001:2006, pjesa A.3.3 Kodi ISPS PVV -5.4.1
Routines for ensuring the integrity of cargo units	Tampering with cargo units.	procedures for monitoring & checking the integrity of cargo units;	ISO 28001:2006, part A.3.3

		procedures for recording, investigating and taking remedial action when unauthorised Access or tampering has been discovered; where appropriate supervision by CCTV.	ISPS Code PVV-5.4.2
Use of seals	Tampering with seals units.	use of container seals that are compliant with ISO/PAS 17712 or other appropriate type of system ensuring the integrity of cargo during transportation; seals stored in a secure location; register of seals is maintained (including used ones); regular reconciliation between register and seals held; - where applicable make arrangements with business partners to check the seals (integrity and numbers) at arrival.	ISO/PAS 17712 PVV 5.4.3
Procedures for inspecting the structure of the cargo unit including ownership of cargo units	Use of hidden places in cargo units for smuggling purposes. To have incomplete control of the cargo units.	- procedures to examine the integrity of the cargo unit prior to loading; - where appropriate use of seven point inspection process (front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage prior to loading); - other kinds of inspections depending on the kind of cargo unit.	ISO 28001:2006, part A.3.3 PVV-5.4.4 and 5.4.5

Maintenance of cargo units	Tampering with cargo units.	- regular programme of routine maintenance; - if maintenance is carried out by a third party, procedures to examine the integrity of the cargo unit after that.	ISO 28001:2006, part A.3.3
Standard operating procedures in case of intrusion and/or tampering with cargo units	No proper action if unauthorised access or tampering.	- appropriate procedures laid down on what measures should be taken when an unauthorised access or tampering is discovered.	ISO 28001:2006, part A.3.3

4.5. Logistical processes

Indicator	Risk description	Possible solutions	References
Active means of transport entering/leaving the customs territory	Lack of control over the transport of goods.	- use of track and trace technology can show unusual stops or delays which could have affected the security of the goods; - special procedures for the selection of carriers/freight forwarders; - make arrangements with business partners to check the seals (integrity and numbers) when the goods arrive at their premises.	PVV -5.5

4.6. Non-fiscal requirements

Indicator	Risk description	Possible solutions	References
Non-fiscal aspects	Ineligible use of goods falling under prohibitions and restrictions or commercial policy measures.	procedures for handling of goods with non-fiscal aspects; appropriate routines and procedures should be established: to distinguish goods subject to non-fiscal requirements and other goods; to check if the operations are carried out in accordance with current (non-fiscal) legislation; to handle goods subject to restrictions/prohibitions/embargo, including dual-use goods; to handle licenses as per the individual requirements. - awareness training/education for staff dealing with goods with non-fiscal aspects.	PVV 5.6

4.7. 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, part 6.2.2 ISO 28001:2007, part A.3.3 PVV -5.7.1
Routines for verifying security measures imposed on others	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	- procedures for ensuring staff are aware of security requirements; - management/supervision checks to ensure the security requirements are complied with.	ISO 28001:2006, part A.3.3 PVV -5.7.2
Supervision for the receipt of goods	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	- personnel assigned to receive the driver on arrival and supervise the unloading of goods; - use pre-arrival information; procedures to ensure assigned staff are present at all times and goods are not left unsupervised perform consistency checks between incoming goods and the transport documents; - for the transportation of secure air cargo/air mail from a known consignor have appropriate systems and procedures in place for checking	ISO 28001:2006, part A.3.3 PVV-5.7.3

		the haulier declaration and identification of the haulier.	
Sealing of incoming goods	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	- procedures for checking the integrity of seals and the correspondence of the seal number with the number in the documents; appointment of designated authorised person.	ISO 28001:2006, part A.3.3 ISO/PAS 17712 PVV 5.7.3
Administrative and physical procedures for the receipt of goods	Lack of control on receipt of goods which may pose a security or safety risk. Introduction, exchange or loss of received goods.	- checks to compare the goods with the accompanying transport and customs documents, picking lists and purchase orders; - checks on completeness by weighing, counting, and tallying and checks on the uniform marking of goods; - updating stock records as soon as possible on arrival; - place goods that pose an anomaly in a specific and secure area and create a process to manage these goods.	ISO 9001:2000, part 7.4 PVV -5.7.4; 5.75; 5.7.6;
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 including reviewing procedures and taking remedial action.	PVV -5.7.7

4.8 Storage of goods

Indicator	Risk description	Possible solutions	References
Assignment of storage location	Inadequate protection of the storage area against external intrusion.	- procedures governing access to the area for storage of goods; - an area or areas is/are designated for the storage of goods with CCTV surveillance system or other appropriate controls.	PVV -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. - Instructions regarding goods notification addressing how and in what way the incoming goods will be checked.	ISO 9001:2001, part 2.2 PVV-5.8.3

Separate storage of different goods	Unauthorised substitution of goods and/or tampering with goods.	- location of goods is recorded in stock records; - where appropriate different goods e. g. goods falling under restrictions or prohibitions, hazardous goods, high value goods, overseas/domestic goods, air cargo are stored separately.	TAPA (Transported Asset Protection Association) Certificate PVV-5.8.4
Additional security and safety measures for access to goods	Unauthorised access to the goods.	- authorised access to the storage area only for designated staff; - visitors and third parties should have temporary identification badges and be accompanied at all time; - data on all visits including names of visitors/third parties, arrival/departure time and attendant should be recorded and stored in appropriate form (e.g. logbook, IT system); - if own storage area is at another operator premises this area should be secured by regular communication between the operators involved and by visits and controls on spot by the AEO.	ISO 28001:2006, part A.3.3 ISPS Code PVV 5.8.5

4.9 Production of goods

Indicator	Risk description	Possible solutions	References
Assignment of production location Additional security and safety measures for access to goods.	Lack of procedures to ensure security and safety of manufactured goods. Unauthorised access to the goods.	- an area is designated for production of goods with appropriate access controls; - authorised access to the production area only for designated staff; - visitors and third parties have to wear high visibility vests and be accompanied at all times; - procedures to ensure safety and security of production processes.	ISO 28001:2006, part A.3. PVV -5.9.2
Internal control procedures	Lack of procedures to ensure security and safety of manufactured goods. Tampering with the goods.	- security processes and procedures should be established to assure the integrity of the production process, e.g. authorised access only for designated staff or appropriately authorised persons, supervision and monitoring of the production process by systems and/or personnel.	ISO 28001:2006, part A.3.3
Packing of products	Incomplete control over the packing of the products. Introduction, exchange or loss of produced goods.	- wherever possible products should be packed in a way that tampering is easily to be detected. An example could be the use of special tape with brand names on it. The tape has to be kept under supervision in that case. Another solution is to use tape which cannot be removed residue-free; - technological aids to packing integrity may also be used e.g. CCTV surveillance, or weight checking;	PVV -5.9.3

		- if possible show the destination of those goods at the latest possible stage (for i.e. bar codes instead of plain text indicating destination).	
Quality inspection	Incomplete control over the flow of goods. Introduction, exchange or loss of produced goods.	- carry out random security and safety checks of produced goods at each stage of production.	

4.10 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 (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.	ISO 28001;2006 part A3.3 PVV-5.10.1
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	- procedures for ensuring staff are aware of customer's security requirements; - Management/supervision checks to ensure the security requirements are complied with.	ISO 28001:2006, part A.3.3 PVV-5.10.3

	registered in a logistical system and of which you don't have any control.		
Supervision over loading of goods	Lack of supervision of loading of goods which might pose a security or safety risk.	- weighing, counting, tallying and uniform marking of goods; - procedures for announcing drivers before arrival; - personnel assigned to receive the driver and supervise the loading of goods; - drivers have no unsupervised access to the loading area; - procedures to ensure assigned staff are present at all times and goods are not left unsupervised; - Appointment of responsible person(s) to carry out checks on routines.	ISO 28001:2006, part A.3 PVV -5.10.4
Sealing of outgoing goods	Sending out goods that are not sealed can lead to introduction, exchange or loss of goods which cannot easily be discovered.	- procedures for controlling, applying, checking and recording seals; - appointment of designated authorised person; - Use of container seals that are compliant with ISO/PAS 17712.	ISO 28001:2006, part A.3.3 ISO/PAS 11712:116 ISO PAS 17712 PVV 5.10.2

Administrative processes of the loading of goods	Delivery of goods which is not registered in a logistical system and of which you don't have any control and thus posing a security or safety risk.	- checks to compare the goods with the accompanying transport and customs documents, loading/packing lists and sales orders; - Updating stock records as soon as possible after departure.	PVV -5.10.5; 5.10.6;
Internal control procedures	No proper action if discrepancies s and/or irregularities are discovered.	- Procedures to record and investigate irregularities e.g. short shipments, broken ant-tampering devices, customer returns, review procedures and take remedial action.	ISO 28001:2006, part A.3.3 PVV-5.10.6

4.11 Security requirements on business partners

Indicator	Risk description	Possible solutions	References
Identification of business partners	Lack of mechanism for clear identification of the business partners.	- procedure in place for identifying regular business partners and unknown clients/customers; - procedures to select and manage business partners where the transport is carried out by a third party; - implement a procedure to select subcontractors based on a list of regular and irregular subcontractors;	

		- subcontractors can be selected on the basis of selection criteria or even of a company specific certification (which can be set up on the base of a certification questionnaire).	
Security requirements imposed on others	Breach of agreed security arrangements with the risk of receiving or delivering unsafe or unsecured goods.	- background checks used to select regular business partners e.g. through the use of internet or rating agencies; - security requirements (e.g. that all goods must be marked, sealed, packed, labelled in a certain way, subject to X-ray checks) are written into contracts with regular business partners; - requirement that contracts will not be further sub-contracted to unknown third parties particularly for the transportation of secure air cargo/air mail; - conclusions provided by experts/external auditors, not related to regular business partners, on complying with security requirements; - evidence that business partners hold relevant accreditations/certificates to prove they comply with international security standards; - procedures for carrying out additional security checks on transactions with unknown or irregular business partners; - reporting and investigation of any security incidents involving business partners and recording remedial action taken.	ISO 28001:2006, part A.3.3 PVV – 5.11

4.12 Personnel security

Indicator	Risk description	Possible solutions	References
Employment policy including for temporary personnel	Infiltration of staff that could pose a security risk.	- background checks on prospective employees, e.g. previous employment history and references; - additional checks on new or existing employees moving to security sensitive posts e.g. police checks on unspent convictions; - requirements on staff to disclose other employment, police cautions/bail, pending court proceedings, or convictions;	ISO 28001:2006, part A.3.3 PVV 5.12.2; 5.12.4

		- periodic background checks/reinvestigations for current personnel; - removal of computer access, return of security pass, keys and/or badge when staff leave or are dismissed; - checks on temporary staff applied at the same standard as permanent staff; - contracts with employment agencies detail level of security checks required; - procedures to ensure employment agencies comply with those standards.	
Level of safety and security awareness of personnel	Lack of proper knowledge on security procedures related to different process (incoming goods, loading, unloading, etc.) with the consequence of accepting/loading/unloading unsafe or insecure goods.	- staff awareness on security measures/arrangements related to different process (incoming goods, loading, unloading, etc.); - set up a register for recording security and	ISO/28001:2006, part A.3.3

		safety anomalies and discuss this with staff on a regular basis; - procedures in place for employees to identify and report suspicious incidents; - pamphlets on security and safety issues can be displayed in specific areas and communicated via a notice-board; - display the security & safety rules in the relevant areas (loading/unloading etc.). The signs must be visible internally (in the sites) and externally (places dedicated to the drivers, temporaries, various partners).	
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;	ISO 28001:2006, part A.3.3 PVV 5.12.3

		- training employees to recognise potential internal threats to security, detection of intrusion/tampering and preventing unauthorised access to secure premises, goods, vehicles, automated systems, seals and records; - conducting tests with “unsafe” goods or occasions; - security and safety training can be part of industrial safety training to outreach all staff; - Security and Safety trainings have to be documented and updated regularly based on happened situations in the company (e.g. every year); - New staff should be trained intensively due to	

		their lack of knowledge and awareness.	

4.12 External services

Indicator	Risk description	Possible solutions	References
External services used for various areas, i.e. packing of products, security, etc.,	Infiltration of staff that could pose a security risk. Incomplete control over the flow of goods	- security requirements e.g. identity checks on employees, restricted access controls are written into contractual agreements; - monitoring compliance with these requirements; use of different badges for external staff; - restricted or controlled access to computer systems; - supervise external services where appropriate; - establish security arrangements and or auditing procedures to ensure the integrity of the goods; - In case of temporary work (i.e. maintenance work) a list of authorised workers of the outsourced company.	ISO 28001:2006, part A.3.3 PVV 5.13

Received by