PD CEN/TR 16412:2012

BSI Standards Publication

Supply chain security (SCS) — Good practice guide for small and medium sized operators

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16412:2012.

The UK participation in its preparation was entrusted by Technical Committee OS/1, Obsolescence management, to Panel OS/1/-/4, Supply chain management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2012

ISBN 978 0 580 77945 9

ICS 03.100.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2012.

Amendments issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16412

September 2012

ICS 03.100.10

English Version

Supply chain security (SCS) - Good practice guide for small and medium sized operators

Sécurité de la chaîne d'approvisionnement - Guide de bonnes pratiques pour les petites et moyennes entreprises

Sicherheit von Lieferketten - Handbuch für bewährte Praktiken für kleine und mittlere Unternehmen

This Technical Report was approved by CEN on 13 August 2012. It has been drawn up by the Technical Committee CEN/TC 379.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TR 16412:2012: E

Contents

Page

Foreword

This document (CEN/TR 16412:2012) has been prepared by Technical Committee CEN/TC 379 “Supply Chain Security”, the secretariat of which is held by NEN.

Supply chains move huge quantities and values of products and services between businesses and between businesses and consumers throughout Europe and between Europe and countries in other continents. These movements present enormous opportunities for organized crime and terrorists. The intrusion of crime and terrorist activity has become a major risk in doing business for the majority of operators within the supply chain, i.e.:

- cargo owners;
- shippers;
- forwarders;
- terminal operators;
- transporters.

1 Scope

This Technical Report aims to provide Small and Medium sized Enterprises (SMEs) basic knowledge about how to manage and mitigate the risk of criminal and terrorist activities. This is a shared objective for the private and public sector.[1] For the private sector, companies have gained experience on measures, which can assist in preventing security breaches from happening, to protect against supply chain interruption. Also some business standards have been developed identifying measures, which companies can execute in order to obtain labels which certify business operations and reward them with a security quality label. The public sector has developed security legislation which companies should either mandatory or voluntary apply into their business operations.

This Guide provides an easy-to-read overview on:

1) How SMEs can apply a supply chain security approach to their operations (Clause 2).

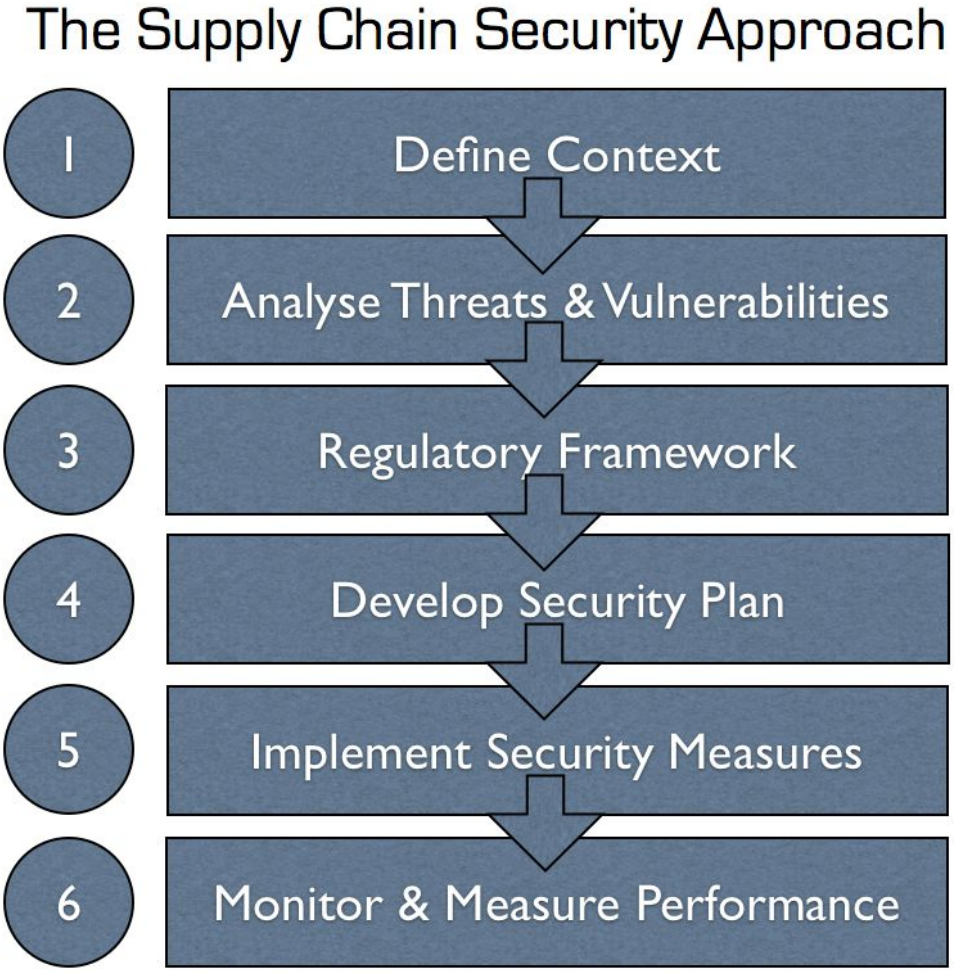
2) The main crime types in the supply chain including some measures to fight these crime types from occurring (Clause 3).

3) Supply chain security legislation and programs, with their respective compliance requirements (Clause 4).

[1] In the context of this guide, “supply chain security” covers risk management, crime prevention, security procedures and technologies, as well as security regulations and programs. The overview and examples in this book are based on recent academic work and interviews with experts in the field, including CEN SCS Feasibility Study (2010); EU FP7-LOGSEC Roadmap (2011) and interviews with CEN TC/379 experts.

2 Recommended Supply Chain Security Approach

How to integrate supply chain security into your business? Various ways are possible and being explored by companies. Existing guidelines and best practices often refer to the exploitation of risk management approaches. However, the practical application of these approaches is often difficult to understand and apply in practice for SMEs. Hence, in this guide a concrete step-by-step approach is explained, with examples of practical security measures to mitigate specific crime risks, and to comply with specific security regulations and standards. In this guide, the following six steps are recommended[2]:


The Supply Chain Security Approach
1
Define Context
2
Analyse Threats & Vulnerabilities
3
Regulatory Framework
4
Develop Security Plan
5
Implement Security Measures
6
Monitor & Measure Performance

FIRST, **define the context** for your supply chain, crime prevention and security management activities. The major questions being:

- Which business are you in, and how "security sensitive" is it?
- Which geographies and transport modes are included?
- Who are the customers, suppliers, insurance providers, governmental agencies and other key stakeholders your supply chain operates with?

As an outcome, you create the context before moving on to the next considerations.

[2] There is no guarantee that a certain security measure brings a sustainable, positive outcome.

SECOND, perform a **threat and vulnerability analysis**, when it comes to actual criminal and terrorist threats in your supply chain. [3] The major questions being:

- Where are the risks of failing today, i.e. where are the gaps calling for enhanced security?
- Which crime types are of particularly high risk in your supply chain? Use statistical sources, if available, while carrying out such risk assessments.
- What are the realized and/or potential consequences of one or more crime incidents?

THIRD, consider **regulatory and program aspects**.[4] The major questions being:

- Which regulations are required for you to operate successfully in your defined business environment, and which programs could support achieving your business objectives?
- What do your customers expect from you? What about your suppliers?
- Have your insurance providers established any requirements?
- What about relevant governmental authorities, including customs and police?

FOURTH, create an overarching **security plan** for your company and/or supply chain, where you consider a variety of security management aspects, taking into consideration the outcomes of your business context; threat and vulnerability; as well as security program and regulatory aspects analysis (steps one, two and three above). The aspects you should take into consideration are:

- Physical security (facilities, vehicles, containers, shipments etc.);
- Data security (in particular systems with supply chain data);
- Human resources security (including selection, training, and exit procedures); - Business partner security (including selection, and auditing); and
- Process control and monitoring of deviations.

FIFTH, choose the **combination of concrete security measures** – investments in technologies, procurement of services, in-house solutions and so forth – and implement them into practice. Embed security procedures and technologies as much as feasible into daily operations, as part of your overall supply chain, logistics, and transport management functions.

SIXTH, monitor and measure the security performance and feedback to the planning cycle. Take corrective actions. Increase security at weak spots, and reduce in the areas where overinvestment has taken place. Pay attention to the dynamics and changing situations when it comes to criminal focus areas and “criminal portfolios”; technical and operational improvements - both licit and illicit aspects - and legislative requirements, and consequences, both for the licit and illicit actors.

[3] Clause 2 helps to increase understanding the types of threats one could be subject to and do something about.

[4] Clause 3 provides an overview of key regulation and programs.

3 Crime prevention in supply chains

3.1 Introduction

Ten relevant crime types have been chosen fallen under the following five categories**:**

1) **Property theft**: Cargo theft; Intellectual property violations.

2) **Targeted damage**: Terrorism; Sabotage.

3) **Cross-border duty and tax fraud**

4) **Illegitimate transporting / importing and/or exporting**: Smuggling of prohibited and restricted goods; People smuggling.

5) **Crime facilitation**: Document forgery; Bogus companies; Cyber crime.

For each crime type, the

- issue (What are the main characteristics and what are the typical products / sectors involved?),
- scope of the problem (Why is it a problem?) and
- actions to take (How to mitigate the risks?)

are being elaborated on.

3.2 Cargo theft

Cargo theft can be defined as "...***any theft of shipment committed during its (surface) transportation or within a warehouse.***"[5]. This covers straightforward theft, hijacking, robbery, fraudulent pick-up, and load diversions, etc.[6]. The value of a single load can be anything from a few thousand to few dozen million Euros. On the other hand, in case of getting caught, cargo crimes often result only in minor legal punishment. Valuable commodities, which have high demand on the after-market and are easily transportable, are quick to sell and particularly vulnerable for cargo theft[7]. These commodities include consumer electronics, cigarettes, food, alcohol, brand apparels, precious metals and prescription drugs. Cargo crime incidents can occur in any part of a supply chain, but truck stops and unsecured parking lots are the most vulnerable spots in the chain (NICB 2010).

In addition to the high financial losses estimated to be over 8 billion Euros in Europe in 2009 [8], the human suffering caused by threats and violence involved in cargo theft is huge.[9] From the private sector perspective, cargo theft is commonly considered the most frequent crime threat in supply chains today. All operators can be usual victims of cargo theft. Manufacturers face material shortages due to theft incidents, resulting in production downtime, missed deliveries and lost sales[10]. For the logistics sector, cargo theft causes liability and insurance problems, lower customer satisfaction and so on. For the **public sector**, cargo theft is a cost

[5] Cargo Theft Report. Applying the Brakes to Road. Cargo Crime in Europe. Public version excluding Appendix D (Europol Restricted). The Hague, 2009. Editorial note: term "surface" is used instead of "road".

[6] Cargo theft is being perceived as an attractive, high reward, low risk criminal industry FIA 2001, Contraband, Organized Crime and the Threat to the Transportation and Supply Chain Function

[7] Felson and Clarke, 1997, Opportunity makes thief

[8] http://www.tapaemea.com/public/

[9] IRU 2006 Attacks on Drivers of International Heavy Goods Vehicles

[10] Anderson, Bill (2007), Securing the Supply Chain – Prevent Cargo Theft, *Security*, Vol. 44, N°5, pp. 56-58

and reputation factor for the police and the legal system. It can be dangerous for consumers, who unknowingly or knowingly buy stolen goods. As yet, fighting cargo crime has not traditionally been a high priority concern for policymakers[11].

Measures to mitigate the risk of theft relate to

- Physical security measures for buildings, parking areas, and vehicles are key.
- Selecting low-risk routes, avoiding unnecessary stops, and not picking up unknown people into trucks are good policies.
- Careful selection and training of personnel and supply chain partners, as well as conducting audits of security capabilities of the logistics service providers normally helps to mitigate the risks.
- (Hidden) tracking devices among the cargo as well as tracking devices in the vehicle – and even vehicle immobilization systems can help to recover the stolen items. [12]
- Training of warehouse workers and drivers can also be a useful recovery measure.

Further **reading** on how to reduce cargo theft in the supply chain:

- *IRU Road Transportation Security Guidelines 2005, which is available at http://www.iru.org/en_guidelines-goods*
- *TAPA FSR 2011 and TAPA TSR 2008, which are available at http://www.tapaemea.com/*

3.3 Counterfeit goods

Counterfeiting can be defined as "***the illegal reproduction or imitation of products, given that this illegality is the result of a violation of any type of intellectual property rights***"[13]. Counterfeits products are mostly transported to affluent markets via legitimate supply chains, whereby the production of the counterfeits often takes place at the upstream of an otherwise legitimate supply chain. Counterfeiting trade can bring huge profits, while there is a low risk of being caught and moderate punishment in case of being caught. In some countries, the public perception is that counterfeiting can be socially acceptable. Advances in technology increasingly give counterfeiters the tools to copy.[14]

It has been estimated that since early 1990s, global trade in counterfeits has increased eight times faster than legitimate trade. Today's global markets for counterfeit products account for 5 % - 7 % of world trade[15]. In a worst-case scenario, counterfeit products can cause serious damage to human health and safety (even death). Medicines, electronics and software remain the most counterfeited products in the world. [16]. Counterfeiting can reduce demand of genuine products resulting in lost sales as well as damage the reputation of the brand owner. This is particularly the case when a customer is deceived and buys a copy thinking it is a real product with proper functionalities and quality. Consumers buy counterfeit products both knowingly and unknowingly.

[11] EC (2003), "Freight transport security", EC Consultation Paper, European Commission, Brussels.

[12] **Detection and recovery** are partially about getting information about an incident as soon and accurately as possible, for both law enforcement and security service centre follow-up.

[13] Nations Interregional Crime and Justice Research Institute (2007). *Counterfeiting: a global spread, a global threat*. Turin: UNICRI.

[14] http://www.iccwbo.org/id399/index.html

[15] World intellectual Property Association, International Anti-counterfeiting Coalition

[16] http://www.havocscope.com/black-market/counterfeit-goods/counterfeit-goods-ranking/

Measures to mitigate the risk of counterfeit goods relate to:

- **Prevention** of counterfeit goods in the supply chain:
  - Close co-operation between the relevant private and public sector actors, i.e. awareness campaigns, development of international agreements and national legislations.
  - Tight contracts with all the supply chain partners to eliminate counterfeit attempts within the (normally) legitimate supply chain.
- **Detection and recovery** relying on capabilities to identify counterfeit products at various stages of the supply chain, in a cost-efficient, non-intrusive and high quality (low false-positives and false-negatives) manner. Measures include:
  - High and low technology means to facilitate the detection process (on product level) including hologram tags, bar codes, micro text and phone help-desks.
  - Monitoring and auditing of consumer sales, auction websites, as well as physical outlets enables detecting (and seizing) counterfeit products.

Further **reading** on how to tackle counterfeit related problems in the supply chain:

- *The International Trademark Association (INTA) and the International Chamber of Commerce (ICC) Business Action to Stop Counterfeiting and Piracy (BASCAP) at http://www.bascap.com/*
- *IP Crime Group: Supply Chain Kit, available at http://www.ipo.gov.uk/ipctoolkit.pdf*

3.4 Terrorism in supply chains

Terrorism can be defined as ***"any act intended to intimidate a population or to compel a government or an international body to act."***[17] Besides destroying (parts of) supply chain itself, terrorism is likely to be connected with a variety of crime types[18] Terrorists may exploit legitimate supply chains to achieve their malicious objectives. Furthermore, terrorist groups can generate profits and fund their operations with legitimate or illicit businesses throughout the supply chain. Terrorist networks may also use of the logistic chain as a conduit to deliver weapons and individual terrorists to a target destination.

Governments across the globe have identified terrorism as unlawful and a major threat to political and social stability. Since 9/11, a large number of counter-terrorism supply chain security initiatives have been launched. These initiatives also impose a challenge for the **private sector operators**[19]. First, they must adapt their operations to a new operating environment with heightened security requirements. Secondly, they have to be prepared to deal with the aftermath of a major terrorist attack. Supply chain operators do not commonly see terrorism as an imminent threat. The bill of anti-terrorist measures imposed by government programmes can be too expensive for companies, especially when these programmes imply monetary investments, or reduce supply chain efficiency as lead times become longer and more unpredictable, i.e. more stringent customs inspection at borders.

[17] http://news.bbc.co.uk/2/hi/americas/4716957.stm

[18] : "To strengthen coordination and cooperation among States in combating crimes that might be connected with terrorism, including drug trafficking in all its aspects, illicit arms trade, in particular of small arms and light weapons, including man-portable air defense systems, money-laundering and smuggling of nuclear, chemical, biological, radiological and other potentially deadly materials." United Nations. General Assembly. The United Nations Global Counter-Terrorism Strategy. A/RES/60/288, Distribution on 20 September 2006.

[19] Sheffi (2001). Supply Chain Management under the Threat of International Terrorism

Measures to mitigate *the risks of terrorism relate to:*

- **Prevention:** focus on access to cargo at any point in the supply chain (cargo integrity).

- **Detection and recovery:** diverse monitoring, detection and inspection solutions can be operated at various stages in the supply chain.

- Contingency and disaster management focus on recovery plans.

Further **reading**:

- *EU-US joint statement on supply chain security, 23.6.2011 http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/eu_us_joint_statement_protocol_en.pdf*

- *World Bank Guidebook in Supply Chain Security , http://siteresources.worldbank.org/INTPRAL/Resources/SCS_Guide_Final.pdf*

3.5 Sabotage in supply chains

Sabotage refers to a "***calculated attack against a predetermined target aiming to damage property, hurt employees, tarnish reputation or disrupt normal business operations***". Motivations for sabotage can be of diverse nature. Frustrated former employees may commit sabotage for revenge. Sabotage can also be used as an instrument for monetary gain and political power. "Professional extortionists" resort to sabotage to give weight to their claims. Political extremists from left to right, environmental activists and fundamentalist religious groups may perpetrate sabotage for political reasons, which makes their activities hard to distinguish from terrorism. Sabotage is also an enabler for other supply chain crimes. Cargo thieves may sabotage power supply in order to shut down electronic security systems. Sabotage itself can be assisted by insider knowledge, identity theft, document fraud and corruption.

A sabotage incident causes harm **for supply chain operators** in terms of cost of damaged assets, lost sales, and a compromised reputation. At worst, sabotage results in a massive product recall campaign resulting in broader financial and reputational losses. This was the case in the UK where 250 000 packets of an over-the-counter painkiller were recalled due to suspected sabotage.[20] Pharmaceutical and food supply chains are particularly prone to sabotage because of their sensitivity to product contamination. Other highly vulnerable sectors include aviation and rail transportation. Sabotage against electronic systems cause major harm for all ICT dependent companies. Sabotage poses a significant risk for citizens and societies as a whole. Threat of product contamination and attacks against infrastructure put citizens' safety in jeopardy, call for increased funding for law enforcement and undermine national competitiveness. **Police** are typically the governmental agency dealing with sabotage cases.

Measures to mitigate the risk of sabotage relate to:

- **Preventing,** i.e. keeping unauthorized companies and persons away from supply chain assets. Special attention should be paid to specific groups of individuals (e.g. recently sacked employees which have shown deep anger) and with specific types of companies (e.g. a competitor who has been placing threats), when it comes to preventing potential sabotage.

- **Detection and recovery**, continuous security, safety and quality monitoring, combined with business contingency plans and teams trained to act in case of sabotage incidents, can be helpful.

[20] http://www.bbc.co.uk/news/health-14685629

More information on anti-sabotage approaches:

- *Defending food and drink - Guidance for the deterrence, detection and defeat of ideologically motivated and other forms of malicious attack on food and drink and their supply arrangements. Available at: http://shop.bsigroup.com/Browse-by-Sector/Food--Drink/PAS-962010/*

- *C-TPAT – Supply Chain Security Best Practice Catalog Available at: www.cbp.gov/linkhandler/cgov/.../ctpat_best_practices.pdf*

3.6 Cross-border duty and tax fraud

The expression ***"the unlawful importation of goods to avoid import duties and taxes"***[21] can be used as a general baseline definition for the illicit avoidance of customs duties and excise taxes in the supply chain. In general terms, **fraud** can be characterised as "***an irregularity committed intentionally with the intention of illicit gain which constitutes a criminal offence***".[22] Duty fraud refers to deliberate evasion of customs duties in legitimate trade articles.

Governments consider tackling fraud as a key objective in protecting financial interests. [23] Duty fraudsters may try to evade customs controls by importing goods through clandestine smuggling routes. They may also transport their goods through legitimate trade lanes and customs checkpoints for example by the aid of fraudulent documentation and/or complicit customs officers. Duty fraud via the legitimate trade lanes is based upon false statements in any convenient data field in the import declaration: i.e. tariff code, value, quantity, country of origin. A dishonest trader can mask a shipment of heavily taxed goods with a cover load of less taxed commodities. Legal consequences of duty fraud include fines, loss of trade licenses and civil charges for liable individuals. Most attractive commodities for duty fraud include high-tax commodities that have a strong and stable demand on the market, including excise taxable goods such as mineral oils, tobacco and alcohol[24]. The biggest (default) liability in duty and excise tax fraud lies with the **importer-of-record**, which may commonly be the cargo owner or shipper. If someone from the **logistics sector** is (knowingly) part of the duty evasion activities, they will naturally be prosecuted. **Governments** are tackling the problem by imposing more stringent regulations on carriers and logistics operators. Customs administration is the main agency that combats duty fraud at a national level.

***Measures to mitigate the risk of duty and tax fraud* relate to prevention, detection and recovery**:

- Awareness creation and training throughout the supply chain, combined with careful selection of own personnel and business partners. Having an anonymous tipping line (phone or email) available to all actors in the chain can act as means of deterrence.

- Risk profiling and targeting IT systems, x-ray and other non-intrusive scanning technologies, random inspections and specific crime-fighting actions such as operations to catch smugglers and fraudsters. (often used by public administrations).

Further **reading** on how to mitigate the risks for customs duty and excise tax fraud:

- *WCO Patterns and Trends report , http://www.mcmullinpublishers.com/downloads/OMD.pdf*

[21] Presentation by EUROPOL, Criminal Finances and Technology Operations Department.

[22] http://ec.europa.eu/anti_fraud/reports/commission/2010/EN.pdf

[23] http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageExcise_ShowContent&propertyType=document&columns=1&id=HMCE_PROD_011637

[24] European Commission – Customs 2002. Good practice Guide.

- *Container Control Programme by UNODC and WCO, http://www.unodc.org/documents/organized-crime/generalbrochureEN.pdf*

3.7 Smuggling of prohibited and restricted goods

Illegal movement of banned or restricted commodities across customs frontiers, is a serious problem in cross-border supply chains. Trade in restricted goods like arms, endangered species and cultural heritage is allowed only under special circumstances[25] whereas banned commodities such as stolen goods, counterfeits, sub-standard food and illegal narcotics can be completely prohibited from being traded and transported. Traffickers have two methods to break bans and restrictions. They can evade all customs controls by transporting their cargo through clandestine routes. The other technique is concealment. Smugglers have proved to be creative in inventing ways to conceal contraband: cannabis inside hollow concrete blocks, elephant tusks hidden behind fake container walls and cultural artefacts concealed among charcoal sacks. Smuggling of prohibited and restricted goods intertwines strongly with other supply chain related crime. Cargo thieves, counterfeiters, poachers and many other antagonists exploit international smuggling networks to transport their illicit cargo to affluent markets. The traffickers themselves may use corruption, cyber crime and fraudulent documents to facilitate the flow of contraband the across borders.

Legitimate supply chain operators are concerned about the possibility that the smugglers exploit their supply chains in their illicit operations. In case authorities detect illegal articles among cargo, a shipment ends up being delayed or confiscated and liable companies are prosecuted.[26] This can cause costs to **cargo owners, shippers and other supply chain operators**. From **governmental** perspective, smuggling of prohibited and restricted goods results in uncontrolled presence of potentially dangerous goods that may put citizen health and safety in jeopardy.

Measures to mitigate the risk of smuggling related to **prevention, detection and recovery:**

- Awareness creation and training throughout the supply chain, combined with careful selection of own personnel and business partners. Having an anonymous tipping line (phone or email) available to all actors in the chain can act as means of deterrence,

- Risk profiling and targeting IT systems, x-ray and other non-intrusive scanning technologies, random inspections and specific crime-fighting actions such as operations to catch smugglers and fraudsters (often used by customs administrations).

Further **reading** on how to mitigate the smuggling risk of prohibited and restricted goods:

- *WCO Patterns and Trends report, http://www.mcmullinpublishers.com/downloads/OMD.pdf*

- *Container Control Programme by UNODC and WCO, http://www.unodc.org/documents/organized-crime/generalbrochureEN.pdf*

[25] http://www.hmrc.gov.uk/customs/banned-restricted.htm

[26] http://www.hmrc.gov.uk/customs/banned-restricted.htm.

3.8 People smuggling

People smuggling can be defined as an activity in which “***smugglers procure, for financial or material gain, the illegal entry of an individual into a country of which he is neither a citizen nor a permanent resident***”[27]. People smuggling is part of organized immigration crime, which covers also human trafficking. In people smuggling criminals assist illegal immigrants to cross borders in exchange of compensation. In human trafficking people are smuggled for exploitation by means of violence, coercion and deception.[28] Legitimate supply chains may be exploited in illicit operations.

Uncontrolled immigration poses a major threat for societies as whole by sparking political conflicts, increasing the power of criminal organizations and disrupting labour market, among other issues. Organized immigration crime causes also problems for all operators in the supply chain. In case authorities detect illegal immigrants among cargo, the shipment is delayed and fines are issued.[28][29] Additional costs can be incurred if e.g. hygiene sensitive cargo such as food and pharmaceuticals are spoiled due to the stowaways.[30]

The measures to mitigate risk of people smuggling relate to:

- **Prevention**: to keep unauthorized individuals and companies away from cargo and transport vehicles. Training and awareness building among staff is a central element in an effective anti-people smuggling strategy.

- **Detection and recovery**: tamper evident container seals, sensors detecting human presence (heart beat, breathing etc.) and the use of canines can be useful.

More information on anti- people smuggling approaches can be found e.g. at:

- *EUROPOL perspective on trafficking in human beings in the European Union. Available at https://www.europol.europa.eu*

- *The UK home office. Organised crime: revenues, economic and social costs, and criminal assets available for seizure. Clauses 2 and 3 deal with people smuggling and human trafficking. The report is available at www.homeoffice.gov.uk*

3.9 Document fraud

Document fraud is a crime where “***forged, altered or dishonestly acquired documents, whether digital or paper-based, are used with intent to commit fraud***”[31]. Forgeries undermine supply chain controls and empower criminals to exploit supply chains for their malicious purposes. By the aid of fraudulent documentation criminals make contraband seem legal merchandise and an unauthorized person authorized. Deception of authorities, business partners and individuals with fraudulent documents often paves the road for more rewarding crime. Cargo thieves capture shipments by presenting convincing but fraudulent contracts of sales. Bogus companies present falsified credentials to build reputation as a reliable business partner. Forged documents play a central role when traffickers smuggle arms, endangered species, stolen goods, counterfeits and other contraband through legitimate supply channels to affluent markets. Smugglers circumvent border control - and at the same time taxes, duties, quotas and embargoes - by submitting false shipping documents

[27] http://www.interpol.org/

[28] UK Home Office: “Organised immigration crime: a post-conviction study”

[29] http://www.telegraph.co.uk/news/uknews/1355984/Driver-who-turned-in-stowaways-is-fined.html

[30] US Department of Transportation, Review of Departmental Actions Concerning the Sanitary Food Transportation Act of 1990, p.4

[31] The creation of a false written document or alteration of a genuine one, with the intent to defraud. (http://legal-dictionary.thefreedictionary.com/forgery)

with misleading claims about trade articles, country of origin and other data entries. Terrorist, dangerous criminals and illegal immigrants move from country to country with the aid of falsified passports, visas and residence permits (OCTA 2011).

The measures to mitigate risk of document fraud relate to:

- **Prevention approaches**: protection of original document templates from unauthorized access and keeping anti-forgery features of the documents confidential.
- **Detection and recovery** approaches: the introduction of anti-forgery features to documents: biometrics, holograms, watermarks, UV reflective inks, RFID tags etc. Effective utilization of document verification technologies and training of personnel are essential in fight against fraudulent documentation

More information on anti –document fraud procedures and solutions is available e.g. at:

- *A good practice guide on pre-employment screening – Document verification by CPNI. Available at www.cpni.gov.uk/documents/*

3.10 Bogus companies

A bogus company can be regarded as *"**setting up a shell company or hijacking a legitimate company to support fraudulent activity.**"*[32] Criminals can set up or take over seemingly legitimate businesses and misuse them for illegal purposes. These so called bogus, shell or front companies can be either appropriately registered companies or officially non-existent representations. Irrespective of their legal status, the purpose of the bogus companies is to enable and cover criminal activities and/or provide a way to launder and re-invest criminal proceedings33. In many cases, the bogus companies disguise their real nature behind fraudulent web sites, licenses, register-of commerce extracts and so on. A bogus company may build a flawless credit history and a trusted relationship with a client and wait for a favourable time and opportunity to trigger a major fraud. This kind of "long con" was the case in the US, where a bogus carrier stole six tractor-trailer loads of tomatoes, right after the market price of tomatoes had surged due to frozen crops.34 A bogus client without a credit history places an order and vanishes without paying right after the goods are delivered. According to the European manufacturers and logistics operators, bogus companies pose an increasing risk for the legitimate businesses. In the supply chain settings, bogus companies are engaged themselves in cargo crime, smuggling of prohibited and restricted goods, duty and excise tax fraud, and organized immigration crime.

Cargo owners and shippers suffer most from the bogus operators. They lose value of stolen goods but also carry costs of re-shipping, litigation against the fraudsters, and increased work related to business partner vetting. Likewise to cargo crime in general, valuable, easily disposable and non-traceable goods are the most attractive targets for bogus companies with intent to steal cargo. Criminals in charge of a bogus company defraud also **transport carriers, freights forwarders and warehouse keepers** by using their services without paying. Bogus companies underpin many criminal activities which cause substantial harm **to the society**: a large scale tax evasion can be enabled by a bogus trading company, human trafficking and smuggling by a fraudulent carrier, illegal dumping of hazardous waste by a dishonest shipping line. Altogether, prevalence of the bogus companies increases power and influence of the criminal organizations in the legal economy.

[32] http://www.actionfraud.org.uk/about-us/who-we-are

[33] Dutch Organized crime assessment

[34] http://www.nytimes.com/2011/04/15/business/15bandits.html?_r=2

The measures to mitigate the risk of bogus companies relate to:

- **Prevention:** Two major measures:
  - Careful business partner selection process, including inspection of credit history, trading record, membership in national trade register of new business partners.
  - Verification of receiver before handover of cargo: authentication of drivers and vehicles entering a terminal.
- **Detection and recovery approaches:** utilization of tracking solutions on the vehicle, container, pallet or piece level (e.g. RFID, GPS and bar code).

More information on how to mitigate the risk of bogus companies can be found e.g. at:

- *Netherlands Police Agency. National Threat Assessment 2008 – Organised crime. Section 5.6. "Misuse of businesses". Available at www.politie.nl.*
- *UK's national fraud reporting centre. "Short and Long Firm Fraud" at Action Fraud website. Available at www.actionfraud.org.uk/fraud.../long_term_and_short_term_fraud*

3.11 Cyber crime

Cyber crime, ***" …include attacks against computer data and systems, identity theft, ... internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets, and various email scams such as phishing."***[35] Modern supply chain management, which is increasingly dependent on IC-Technologies that enable supply chain operators to increase productivity and cut down costs, is increasingly vulnerable to cyber crime.

A successful cyber attack endangers business continuity, puts shipments at risk and undermines credibility. Access to a company's information system allows a cyber attacker the opportunity to damage, alter or steal data. The intruder may sabotage business operations by crashing the system or altering information. Alternatively, the cyber criminal may sell confidential data further to other criminal groups specialized in traditional off-line crime. For instance, cargo thieves benefit greatly from information about transportation schedules and bills of ladings. Consequences of cyber crime can be serious. Therefore different supply chain operators regard cyber crime as one of the most serious threats to supply chains. It appears that cyber crime has evolved from the ego-boosting vandalism towards professional profit generating activity. Career criminals making their living with ICT-related crime are often not discouraged nor deterred by new security software or increased law enforcement activities. Cyber crime is an international activity perpetrated by criminals who look after their anonymity. This makes policing, investigation and prosecution of the cyber criminals extremely difficult. Cyber crime also evolves quickly, hand-in-hand with rapid technological development.

Measures to mitigate the risk of cyber crime relate to:

- Prevention: Up-to-date IT security measures including firewalls, encryption, identity management systems, Secure Socket Layers (SSL), application authentication, virtual private networks**.**
- **Detection and recovery approaches:** constant monitoring and controlling of IT systems with appropriate software which is able to detect a variety of malwares including key loggers, Trojan horses, spy bots and so on.

Cyber crime is **explored further** e.g. in following references:

- *EUROPOL. Internet facilitated organized crime iOCAT. Available at https://www.europol.europa.eu.*

[35] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

- *ISO/IEC 27002:2005. Information technology -- Security techniques -- Code of practice for information security management. Available at http://www.iso.org/.*

4 Supply chain security regulations and programs

4.1 Introduction

Supply chain security regulations and programs have been designed to fight against one or more types of criminal (and terrorist) activities in the supply chain. Security programs are driven by governments and by the private sector; and regulations (naturally) by governmental law making and enforcement systems.

For the purpose of this Good Practice Guidebook, following previous work done e.g. CEN SCS Feasibility Study (2010) and FP7-LOGSEC Supply Chain Security Roadmap (2011), seven security initiatives, categorized in three intuitive groups, have been chosen for brief analysis and presentation purposes:

- Mandatory data requirements: ICS/ECS
- Company level binding regulations: Maritime security regulations, Aviation security regulations
- Company level voluntary certification: EU AEO, Regulated agent / Known consignor / Account consignor, ISO 28000, TAPA

For each of the seven security initiatives, the following is explained:

- What is the initiative all about and whom is it meant for?
- What are some of the basic requirements and implications?

4.2 Import Control System (ICS) and Export Control System (ECS) in the EU

Import Control System (ICS) is a ***systems architecture developed by the Community for the lodging and processing of Entry Summary Declarations, and for the exchange of messages between national customs administrations and between them and economic operators and with the European Commission.***[36] ICS obliges **carriers or their representatives** to submit pre-arrival information for all cargo entering EU territory for shipment risk analysis purposes. The advanced information must be provided in the form Entry Summary Declaration (ESD) that includes among other things details about contents of cargo, planned routing and traders involved with the movement of the goods[37][38]. Time limits for lodging the EDS to a customs system vary between modes of transportation. In case of containerized maritime cargo, cargo information must be submitted 24 hours before loading at the port of origin[39] whereas in road transportation the ESD must be sent at least one hour prior arriving at the customs checkpoint.[40] Operators failing to comply with the ICS regulation face potentially fines, sanctions and delays at the borders.

Export Control System (ECS) introduces EU ***procedures to computerize and control indirect exports41 and to implement the EU safety and security regulations***[42]. ECS is the first stage of an Automated Export

[36] http://ec.europa.eu/ecip/help/faq/ens7_en.htm#faqsection

[37] FAQ's: Import Control System (ICS) – Information for UK Traders. Available at http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageImport_ShowContent&id=HMCE_PROD1_030208&propertyType=document

[38] Annex 30A of Commission Regulation 1875/2006 lists required data elements of the ESD

[39] Referred sometimes as the "EU 24 Hour Rule"

[40] http://www.ics-import-control-system.net/ICS-reglementation.html

[41] Where an export leaves the EU from a Member State (MS) other than the MS of export

[42] Set out in the European Parliament and Council Regulation (EC) No 648/2005 and the Commission Regulation 1875/2006/EC.

System (AES) aiming for a computerized EU export system to common standards.[43] Just like with ICS, the responsibility to file the required data within the required time schedule lies **with the carrier**, or another person with the carrier's knowledge and consent.

4.3 Maritime Security Legislation, ISPS Code in the EU

International regulations to ensure the security of maritime transportation are being issued by the International Maritime Organization, IMO, in the International Ship and Port Facility Security, ISPS, code[44]. The code contains minimum security requirements for ships, ports and government agencies and is in force since July 1, 2004. Four main articles in the code highlight how security enhancements may be achieved:[45]

- **Article TP33/10 Access to premises.** The code suggests the usage of signs, fences and barriers to prevent the unauthorized access to the port premises.

- **Article TP34/10 Compliance with international security requirements.** Ships entering a port are requested to comply with the security requirements for signs and port facilities.

- **Article TP35/10 Notification with respect to security.** The article states the necessity to request permission to enter a port by means of a pre-arrival report.

- **Article TP36/10 Security control of ships in ports.** This article authorizes port authorities to perform inspections on the ships**.**

In the European context, the ISPS-based relevant legislations on maritime security consist of[46]:

- **Regulation (EC) No 725/2004** on enhancing ship and port facility security

- Port Security Directive : **Directive 2005/65/EC** on enhancing port security

- Commission inspections in the field of maritime security: **Commission Regulation (EC) No 324/2008** on procedures for conducting Commission inspections in the field of maritime security.

ISPS code, and the EU legislation, is mandatory for **shipping lines and port terminal operators**, requiring them to invest e.g. in *sea-side and land-side traffic management and access control equipment, systems, IT, procedures and/or security personnel.* It does not have direct impacts on **freight forwarders, manufacturers, shippers and cargo owners**.

4.4 Aviation Security Legislation, Air Cargo Supply Chains in the EU

According to the European Commission, ***security has been a matter of concern for civil aviation for several decades, but in particular since the bombing of a flight above Lockerbie in 1988. However, aviation security has, up until more recently, been addressed on essentially a national level.*** EC also notes that at the international level, though for some time Standards and Recommended Practices have been laid down by the International Civil Aviation Organisation (ICAO) for States to implement, these are not regulated by a binding mechanism to guarantee their full and proper application.[47] Following the terrorist attacks in the United States on 11 September 2001 when commercial aircraft were used as weapons of mass

[43] http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageImport_ShowContent&propertyType=document&id=HMCE_MIG_009926

[44] An amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988), Chapter XI-2.

[45] IMO (2011), Maritime Security, http://www5.imo.org/SharePoint/mainframe.asp?topic_id=551

[46] http://ec.europa.eu/transport/maritime/security/doc/legislation_maritime_security.pdf

[47] http://ec.europa.eu/transport/air/security/security_en.htm

destruction, the Commission made a legislative proposal to bring aviation security under the EU's regulatory umbrella[48][49].

Today, ***three* categories of aviation security legislation** exist in the EU[50]: Framework regulation[51]; supplementing regulations[52]; and implementing regulations.[53] Examples of security requirements set by current European regulations include the following ones:

- **Airport security**: boundaries; security restricted areas; access control; identification cards; vehicle passes; security patrols etc.
- **Protection of aircraft**: security searches; and general and specific protection measures.
- **Cargo and mail**: security controls; cargo screening; protection of cargo and mail during transport; protection of cargo and mail at the airport etc.
- **Staff recruitment and training**: security controls; supervision of other employees etc.
- **Security equipment**: standards, approval process etc.

When it comes to the mandatory requirements set by the aviation security regulations, they influence the variety of **operators** within the “extended airport community”. The simple benefit if that by complying these regulations, the companies can legally operate in their respective businesses.

4.5 European Union Authorized Economic Operator (EU AEO)

The World Customs Organization (WCO) in the SAFE Framework of Standards considers Authorized Economic Operator (EU AEO) to be “***a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs Administration as complying with WCO or equivalent supply chain security standards.*** According to the WCO, “***AEOs include inter alia manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors***”.[54]

The European Union, **EU AEO certification** is available in following three versions:

[48] http://ec.europa.eu/transport/air/security/security_en.htm

[49] This initiative led to the adoption of framework Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security and thus provided the basis for allowing harmonisation of aviation security rules across the European Union with binding effect.

[50] http://ec.europa.eu/transport/air/security/legislation_en.htm

[51] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002

[52] For example Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council

[53] For example Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security

[54] WCO SAFE Framework of Standards, June 2007, p.6.

- **Customs Simplifications (AEO-C).** To obtain this certification operators have to show appropriate record-keeping and financial solvency.[55]

- **Security and Safety (AEO-S).** In addition to the AEO-C requirements, operators need to show their capacity to maintain appropriate safety and security standards.

- **Customs Simplifications/Security and Safety (AEO-F).** This is the highest level of certification and basically to obtain this status the operators have to fulfill with the AEO-C and AEO-S criteria.

The **EU AEO Guidelines, Section V**, contains a questionnaire providing a list of points for attention to assist both customs authorities and economic operators to assess whether the AEO criteria are met or not.[56] The questionnaire has following 13 sub-sections: *Security (self)assessment; Entry and access to premises; Physical security; Cargo units; Logistical processes; Non-fiscal requirements; Incoming goods; Storage of goods; Production of goods; Loading of goods; Security requirements business partners; Personnel security; and External services*.[57]

AEO-S and AEO-F certificate is issued to any economic operator established in the Community who fulfils the criteria of customs compliance, appropriate record-keeping standards, financial solvency, and maintains appropriate security and safety standards. The security and safety standards are described in Section V.[58] Both **cargo owners as well as logistics companies** can apply for EU AEO, in case they have direct involvement in international (beyond EU-borders) trade and/or logistics. Ultimately, the concept AEO should simplify customs clearance for economic operators while also making it possible to implement customs controls more efficiently and in a more targeted manner and to tighten authorization procedures for customs simplifications.[59]

4.6 Regulated agent, Known consignor and Account consignor in the EU

Specific “trusted trader” status - regulation-based, voluntary to implement – exist in the European air cargo supply chains, in particular the following three[60][61]:

- **Regulated agent**: an air carrier, agent, freight forwarder or any other entity who ensures security controls in respect of cargo or mail;

- **Known consignor**: a consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of cargo or mail on any aircraft;

- **Account consignor**: a consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of that cargo on all-cargo aircraft or mail on all-mail aircraft;

[55] Editorial note: if a company only applies or has AEO-C status, one could argue that it is out-of-scope for this guidebook; however, as this guidebook has chosen a broader ”anti-crime” approach to supply chain security, even AEO-C as a stand-alone is considered to be about prevention of duty fraud, i.e. part of supply chain security.

[56] Note: there is more than one-way to address the issues specified in the questionnaire: the same requirements can be complied with using different means and methods.

[57] http://ec.europa.eu/ecip/documents/who_is/aeo_guidelines_en.pdf

[58] http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/aeo_guidelines_en.pdf , p.7

[59] http://english.bmf.gv.at/Customs/Trade/Securityregulations_474/_start.htm

[60] COMMISSION REGULATION (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security.

[61] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:055:0001:0055:EN:PDF

The actual security requirements include *security at premises; security controls; protection of cargo during transportation; and protection of cargo at airports,* amongst other requirements. Regulated agent status typically applies only to **logistics sector**, while Known consignor and Account consignor may apply for both **logistics and shipper/cargo owner sectors**. As the main **benefit** for businesses to such statuses, cargo originated from such "trusted sources", are in principle subject to less security controls during the "last mile" operations.

4.7 ISO 28000 Series of Standards on Supply Chain Security Management Systems

According to the International Standards Organization (ISO), the **ISO 28000 series of standards** on supply chain security management systems ***has the aim to reduce risks to people and cargo within the supply chain.*** Moreover, the standards ***address potential security issues at all stages of the supply process, thus targeting threats such as terrorism, fraud and piracy***."[62] Standards include the following five:

- **ISO 28000:2007** Specification for security management systems for the supply chain;
- **ISO 28001:2007** Security management systems for the supply chain – Best practices for implementing supply chain security – Assessments and plans – Requirements and guidance;
- **ISO 28002:2011** Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
- **ISO 28003:2007** Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems;
- **ISO 28004:2007** Security management systems for the supply chain – Guidelines for the implementation of ISO 28000.

The series includes provisions to: establish, implement, maintain and improve a security management system; assure conformity with security management policy and demonstrate such conformity; seek certification/registration of conformity by an accredited third party organization; and/or make a self-determination and self-declaration of conformity.[63] According to ISO, the standards can be applied by organizations involved in **manufacturing, service, storage or transportation by air, rail, road and sea at any stage of the production or supply process**, i.e. by virtually all actors in the supply chain.

4.8 Transported Asset Protection Association (TAPA) in Europe

The **Transported Asset Protection Association (TAPA),** according to their communication materials, ***represents businesses fighting back against cargo crime that want to use real-time intelligence and the latest preventative measures to protect goods in the supply chain***. Moreover, TAPA is a ***forum uniting global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains.***[64] TAPA has introduced the following four sets of security requirements and standards in the supply chain[65]:

- **Freight Security Requirements** (FSR) - Established to ensure the safe and secure in-transit storage and warehousing of any TAPA members' assets throughout the world.

[62] Slightly modifed from: http://www.iso.org/iso/pressrelease.htm?refid=Ref1086

[63] Slightly modifed from: http://www.iso.org/iso/pressrelease.htm?refid=Ref1086

[64] http://www.tapaemea.com/download/TAPA_Brochure.pdf?PHPSESSID=7619991b32189f73b8cba51512489c1e

[65] http://www.tapaemea.com/download/TAPA_Brochure.pdf?PHPSESSID=7619991b32189f73b8cba51512489c1e , p.3

- **Trucking Security Requirements** (TSR) - Specifies the minimum acceptable security standards for assets traveling throughout the supply chain and the methods to be used in maintaining those standards.

- **Parking Security Requirements** (PSR).

- **TAPA Air Cargo Security Standards** (TACSS).

As an example, **FSR addresses supply chain security** in terms of: Perimeter Security; Access Control – Office Areas; Facility Dock/Warehouse; Security Systems; Security Procedures; Standard Truck Security Requirements; Pre-Alerts; and Enhanced Security Requirements. TAPA members consist of high value goods manufacturers / distributors; logistics sector; insurers; and organizations that support TAPA aims. From compliance perspective, it is **the logistics sector – especially transport companies and warehouse keepers** – who may choose to comply with one or more of the TAPA requirements / standards; by the request of their customers, i.e. cargo owners and shippers.

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™