



BSI Standards Publication

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

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.

© The British Standards Institution 2012

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

© 2012 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

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

AVA Documents
Document Sharing Hub

Contents

Page

Foreword.....	3
1 Scope	4
2 Recommended Supply Chain Security Approach.....	5
3 Crime prevention in supply chains	7
3.1 Introduction	7
3.2 Cargo theft.....	7
3.3 Counterfeit goods	8
3.4 Terrorism in supply chains.....	9
3.5 Sabotage in supply chains	10
3.6 Cross-border duty and tax fraud.....	11
3.7 Smuggling of prohibited and restricted goods	12
3.8 People smuggling	13
3.9 Document fraud	13
3.10 Bogus companies	14
3.11 Cyber crime	15
4 Supply chain security regulations and programs	17
4.1 Introduction	17
4.2 Import Control System (ICS) and Export Control System (ECS) in the EU	17
4.3 Maritime Security Legislation, ISPS Code in the EU.....	18
4.4 Aviation Security Legislation, Air Cargo Supply Chains in the EU	18
4.5 European Union Authorized Economic Operator (EU AEO)	19
4.6 Regulated agent, Known consignor and Account consignor in the EU	20
4.7 ISO 28000 Series of Standards on Supply Chain Security Management Systems.....	21
4.8 Transported Asset Protection Association (TAPA) in Europe.....	21

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:

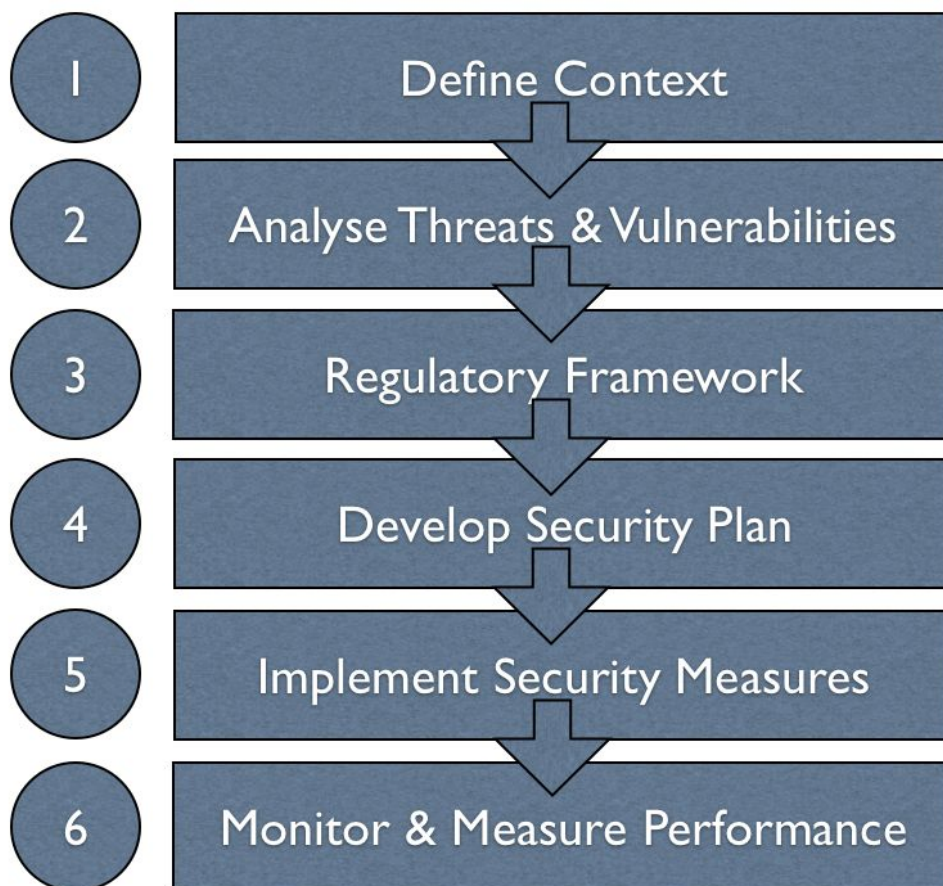
- 1) How SMEs can apply a supply chain security approach to their operations (Clause 2).
- 2) The main crime types in the supply chain including some measures to fight these crime types from occurring (Clause 3).
- 3) Supply chain security legislation and programs, with their respective compliance requirements (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 recommended²:

The Supply Chain Security Approach



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.