TARNEAHELA TURVALISUSE JUHTIMISSÜSTEEMID
Juhised ISO 28000 rakendamiseks
Osa 1: Üldpõhimõtted

Security management systems for the supply chain
Guidelines for the implementation of ISO 28000
Part 1: General principles
(ISO 28004-1:2007)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-ISO 28004-1:2009 „Tarneahela turvalisuse juhtimissüsteemid. Juhised ISO 28000 rakendamiseks. Osa 1: Üldpõhimõtted“ sisaldab rahvusvahelise standardi ISO 28004-1:2007 „Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles“ ja selle paranduse ISO 28004-1:2007/Cor 1:2012 modifitseeritud ingliskeelset teksti.	This Estonian Standard EVS-ISO 28004-1:2009 consists of the modified English text of the International Standard ISO 28004-1:2007 “Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles” including its corrigendum ISO 28004-1:2007/Cor 1:2012.
Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 33, standardi avaldamist on korraldanud Eesti Standardikeskus.	Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 33, the Estonian standard has been published by the Estonian Centre for Standardisation.
Standard EVS-ISO 28004-1:2009 on jõustunud sellekohase teate avaldamisega EVS Teataja 2009. aasta veebruarikuu numbris.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

See rahvusvaheline standard annab üldisi juhiseid standardi ISO 28000:2007 („Tarneahela turvalisuse juhtimissüsteemide spetsifikatsioon“) kohaldamiseks.

See standard selgitab ISO 28000 aluspõhimõtteid ja kirjeldab ISO 28000 iga nõude eesmärki, tüüpilisi sisendeid, protsesse ja tüüpilisi väljundeid. Tegemist on abivahendiga ISO 28000 mõistmiseks ja elluviimiseks.

Standard ei sisalda täiendavaid nõudeid lisaks standardis ISO 28000 sätestatud nõuetele ega näe ette kohustuslikke lähenemisviise ISO 28000 elluviimisele.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 47.020.99

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 28004 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

This first edition of ISO 28004 cancels and replaces ISO/PAS 28004:2006, which has been technically revised.

Introduction

ISO 28000:2007, *Specification for security management systems for the supply chain,* and this International Standard have been developed in response to the need for a recognizable supply chain management system standard against which their security management systems can be assessed and certified and for guidance on the implementation of such a standard.

ISO 28000 is compatible with the ISO 9001:2000 (Quality) and ISO 14001:2004 (Environmental) management systems standards. They facilitate the integration of quality, environmental and supply chain management systems by organizations, should they wish to do so.

This International Standard includes a box at the beginning of each clause/subclause, which gives the complete requirements from ISO 28000; this is followed by relevant guidance. The clause numbering of this International Standard is aligned with that of ISO 28000.

This International Standard will be reviewed or amended when considered appropriate. Reviews will be conducted when ISO 28000 is revised.

This International Standard does not purport to include all necessary provisions of a contract between supply chain operators, suppliers and stakeholders. Users are responsible for its correct application.

Compliance with this International Standard does not of itself confer immunity from legal obligations.

Security management systems for the supply chain — Guidelines for the implementation of ISO 28000

1 Scope

This International Standard provides generic advice on the application of ISO 28000:2007, *Specification for security management systems for the supply chain*.

It explains the underlying principles of ISO 28000 and describes the intent, typical inputs, processes and typical outputs, for each requirement of ISO 28000. This is to aid the understanding and implementation of ISO 28000.

This International Standard does not create additional requirements to those specified in ISO 28000, nor does it prescribe mandatory approaches to the implementation of ISO 28000.

ISO 28000

1 Scope

This International Standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

This International Standard is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

a) establish, implement, maintain and improve a security management system;

b) assure compliance with stated security management policy;

c) demonstrate such compliance to others;

d) seek certification/registration of its security management system by an Accredited third party Certification Body; or

e) make a self-determination and self-declaration of compliance with this International Standard.

There are legislative and regulatory codes that address some of the requirements in this International Standard.

It is not the intention of this International Standard to require duplicative demonstration of compliance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.

2 Normative references

No normative references are cited. This clause is included in order to retain clause numbering similar to ISO 28000.

3 Terms and definitions

ISO 28000

3 Terms and definitions

3.1
facility
plant, machinery, property, buildings, vehicles, ships, port facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service

NOTE This definition includes any software code that is critical to the delivery of security and the application of security management.

3.2
security
resistance to intentional, unauthorized act(s) designed to cause harm or damage to or by, the supply chain

3.3
security management
systematic and coordinated activities and practices through which an organization optimally manages its risks and the associated potential threats and impacts there from

3.4
security management objective
specific outcome or achievement required of security in order to meet the security management policy

NOTE It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.

3.5
security management policy
overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements

3.6
security management programmes
means by which a security management objective is achieved

3.7
security management target
specific level of performance required to achieve a security management objective

3.8
stakeholder
person or entity having a vested interest in the organization's performance, success or the impact of its activities

NOTE Examples include customers, shareholders, financiers, insurers, regulators, statutory bodies, employees, contractors, suppliers, labour organizations or society.