Tarneahela turvalisuse tagamise juhtimissüsteemid Parimad viisid tarneahela turvalisuse tagamiseks, hinnangud ja plaanid Nõuded ja juhised

Security management systems for the supply chain
Best practices for implementing supply chain security, assessments and plans
Requirements and guidance

EESTI STANDARDIKESKUS EVS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
Käesolev Eesti standard EVS-ISO 28001:2009 “Tarneahela turvalisuse tagamise juhtimissüsteemid. Parimad viisid tarneahela turvalisuse tagamiseks, hinnangud ja plaanid. Nõuded ja juhised” sisaldab rahvusvahelise standardi ISO 28001:2007 “Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance” identset ingliskeelset teksti.	This Estonian Standard EVS-ISO 28001:2009 consists of the identical English text of the International Standard ISO 28001:2007 “Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance”.
Ettepaneku rahvusvahelise standardi ümbertrükimeetodil ülevõtuks esitas EVS/TK 33 ”Juhtimissüsteemid”, standardi avaldamise korraldas Eesti Standardikeskus.	Proposal to adopt the International Standard by reprint method was presented by EVS/TK 33 ”Management Systems", Estonian standard is published by the Estonian Centre for Standardisation.
Standard EVS-ISO 28001:2009 on kinnitatud Eesti Standardikeskuse 14.01.2009 käskkirjaga nr 9 ja jõustub sellekohase teate avaldamisel EVS Teataja 2009. aasta veebruarikuu numbris.	This standard is ratified with the order of Estonian Centre for Standardisation dated 14.01.2009 No. 9 and is endorsed with the notification published in the February 2009 edition of official bulletin of the Estonian national standardisation organisation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from Estonian Centre for Standardisation.
Käsitlusala	**Scope**
Käesolev rahvusvaheline standard sisaldab nõudeid ja juhiseid rahvusvahelise tarneahela ettevõtetele, selleks et	This International Standard provides requirements and guidance for organizations in international supply chains to
— arendada ja rakendada tarneahela turvalisuse protsesse; — tagada ja dokumenteerida tarneahela või selle osa turvalisus minimaalsel tasemel;	— develop and implement supply chain security processes; — establish and document a minimum level of security within a supply chain(s) or segment of a supply chain;
— aidata tagada vastavus kehtivatele volitatud ettevõtja (AEO – authorized economic operator) kriteeriumitele, mida esindab Maailma Tolliorganisatsiooni standardite süsteem, ning rahvuslikele tarneahela turvalisuse programmidele.	— assist in meeting the applicable Authorized Economic Operators criteria set forth in the World Customs Organization Framework of Standards and conforming national supply chain security programmes.
MÄRKUS Üksnes osalev rahvuslik tolliagentuur saab määrata ettevõtteid AEO-deks vastavalt tarneahela turvalisuse programmile ja tema sertifitseerimise ja valideerimise nõuetele.	NOTE Only a participating National Customs Agency can designate organizations as Authorized Economic Operators in accordance with its supply chain security programme and its attendant certification and validation requirements.
Lisaks sellele esitab käesolev rahvusvaheline standard kindlad dokumenteerimise nõuded, mis võimaldavad ehtsust kontrollida.	In addition, this International Standard establishes certain documentation requirements that would permit verification.
Käesoleva rahvusvahelise standardi kasutajad	Users of this International Standard will
— määravad kindlaks rahvusvahelise tarneahela osa, mille ulatuses nad peavad tagama turvalisuse (vaata 4.1); — viivad läbi turvalisuse hindamisi selles tarneahela osas ning arendavad välja vajalikke vastumeetmeid; — arendavad ja rakendavad tarneahela turvalisuse plaani;	— define the portion of an international supply chain they have established security within (see 4.1); — conduct security assessments on that portion of the supply chain and develop adequate countermeasures; — develop and implement a supply chain security plan;

— koolitavad turvapersonali nende turvalisusega seotud kohustuste alal.	— train security personnel in their security related duties.

ICS 47.020.99 Muud laevaehituse ja mereehitistega seotud standardid

Võtmesõnad: juhtimissüsteemid

Taotluslikult tühjaks jäetud

Contents

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 28001 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 28001 cancels and replaces ISO/PAS 28001:2006, which has been technically revised.

Introduction

Security incidents against international supply chains are threats to international trade and the economic growth of trading nations. People, goods, infrastructure and equipment — including means of transport — need to be protected against security incidents and their potentially devastating effects. Such protection benefits the economy and society as a whole.

International supply chains are highly dynamic and consist of many entities and business partners. This International Standard recognizes this complexity. It has been developed to allow an individual organization in the supply chain to apply its requirements in conformance with the organization's particular business model and its role and function in the international supply chain.

This International Standard provides an option for organizations to establish and document reasonable levels of security within international supply chains and their components. It will enable such organizations to make better risk-based decisions concerning the security in those international supply chains.

This International Standard is multimodal and is intended to be in concert with and to complement the World Customs Organization's Framework of Standards to secure and facilitate global trade (Framework). It does not attempt to cover, replace or supersede individual customs agencies' supply chain security programmes and their certification and validation requirements.

The use of this International Standard will help an organization to establish adequate levels of security within those part(s) of an international supply chain which it controls. It is also a basis for determining or validating the level of existing security within such organizations' supply chain(s) by internal or external auditors or by those government agencies that choose to use compliance with this International Standard as the baseline for acceptance into their supply chain security programmes. Customers, business partners, government agencies and others might request organizations which claim compliance with this International Standard to undergo an audit or a validation to confirm such compliance. Government agencies might find it mutually agreeable to accept validations conducted by other governments' agencies. If a third-party organization audit is to be conducted, then the organization needs to consider employing a third-party certification body accredited by a competent body, which is a member of the International Accreditation Forum (see Annex C).

It is not the intention of this International Standard to duplicate governmental requirements and standards regarding supply chain security in compliance with the WCO SAFE Framework. Organizations that have already been certified or validated by mutually recognizing governments are compliant with this International Standard.

Outputs resulting from this International Standard will be the following.

— A Statement of Coverage that defines the boundaries of the supply chain that is covered by the security plan.

— A Security Assessment that documents the vulnerabilities of the supply chain to defined security threat scenarios. It also describes the impacts that can reasonably be expected from each of the potential security threat scenarios.

— A Security Plan that describes security measures in place to manage the security threat scenarios identified by the Security assessment.

— A training programme setting out how security personnel will be trained to meet their assigned security related duties.

To undertake the security assessment needed to produce the security plan, an organization using this International Standard will

- identify the threats posed (security threat scenarios);
- determine how likely persons could progress each of the security threat scenarios identified by the Security Assessment into a security incident.

This determination is made by reviewing the current state of security in the supply chain. Based on the findings of that review, professional judgment is used to identify how vulnerable the supply chain is to each security threat scenario.

If the supply chain is considered unacceptably vulnerable to a security threat scenario, the organization will develop additional procedures or operational changes to lower likelihood, consequence or both. These are called countermeasures. Based upon a system of priorities, countermeasures need to be incorporated into the security plan to reduce the threat to an acceptable level.

Annexes A and B are illustrative examples of risk management based security processes for protecting people, assets and international supply chain missions. They facilitate both a macro approach for complex supply chains and/or more discrete approaches for portions thereof.

These annexes are also intended to

- facilitate understanding, adoption and implementation of methodologies, which can be customized by organizations;
- provide guidance for baseline security management for continual improvement;
- assist organizations to manage resources to address existing and emerging security risks;
- describe possible means for assessment of risk and mitigation of security threats in the supply chain from raw materiel allocation through storage, manufacturing and transportation of finished goods to the market place.

Annex C provides guidance for obtaining advice and certification for this International Standard if an organization using it chooses to exercise this option.

Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

1 Scope

This International Standard provides requirements and guidance for organizations in international supply chains to

- develop and implement supply chain security processes;
- establish and document a minimum level of security within a supply chain(s) or segment of a supply chain;
- assist in meeting the applicable authorized economic operator (AEO) criteria set forth in the World Customs Organization Framework of Standards and conforming national supply chain security programmes.

NOTE Only a participating National Customs Agency can designate organizations as AEOs in accordance with its supply chain security programme and its attendant certification and validation requirements.

In addition, this International Standard establishes certain documentation requirements that would permit verification.

Users of this International Standard will

- define the portion of an international supply chain within which they have established security (see 4.1);
- conduct security assessments on that portion of the supply chain and develop adequate countermeasures;
- develop and implement a supply chain security plan;
- train security personnel in their security related duties.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 20858:—[1], *Ships and marine technology — Maritime port facility security assessments and security plan development*

[1] To be published. Revision of ISO/PAS 20858:2004.