

Specification for security management systems for the supply chain

ICS 47.020.99

National foreword

This Draft for Development reproduces verbatim ISO/PAS 28000:2005.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature because it is still under development and, with insufficient data as yet to relate it to experience in the field, it may be subject to significant change. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

A PAS is a Technical Specification not fulfilling the requirements for a standard, but made available to the public and established in an organization operating under a given procedure.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for the Technical Specification. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status at the end of its 3-year life. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international standard, to extend the life of the Technical Specification for another 3 years or to withdraw it. Comments should be sent in writing to the Secretary of BSI Technical Committee SME/32, Ships and marine technology, at British Standards House, 389 Chiswick High Road, London W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

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

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

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

Compliance with a Draft for Development does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/PAS title page, pages ii to vi, pages 1 to 16, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 30 January 2006

© BSI 30 January 2006

ISBN 0 580 47391 0

PUBLICLY
AVAILABLE
SPECIFICATION

**ISO/PAS
28000**

First edition
2005-11-15

**Specification for security management
systems for the supply chain**

*Spécifications pour les systèmes de management de la sûreté pour la
chaîne d'approvisionnement*



Reference number
ISO/PAS 28000:2005(E)

AVA Documents
Document Sharing Hub

Contents		Page
Foreword.....		iv
Introduction		v
1	Scope.....	1
2	Normative references	1
3	Terms and definitions	1
4	Security management system elements.....	3
4.1	General requirements	3
4.2	Security management policy	4
4.3	Security risk assessment and planning	4
4.4	Implementation and operation.....	7
4.5	Checking and corrective action.....	10
4.6	Management review and continual improvement.....	12
Annex A (informative) Correspondence between ISO/PAS 28000:2005, ISO 14001:2004 and ISO 9001:2000		13
Bibliography		16

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.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;
- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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/PAS 28000 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.

Introduction

This Publicly Available Specification has been developed in response to demand from industry for a security management standard. Its ultimate objective is to improve the security of supply chains. This Publicly Available Specification is a high level management standard that enables an organization to establish an overall supply chain security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs. Since supply chains are dynamic in nature, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management as illustrated in Figure 1.

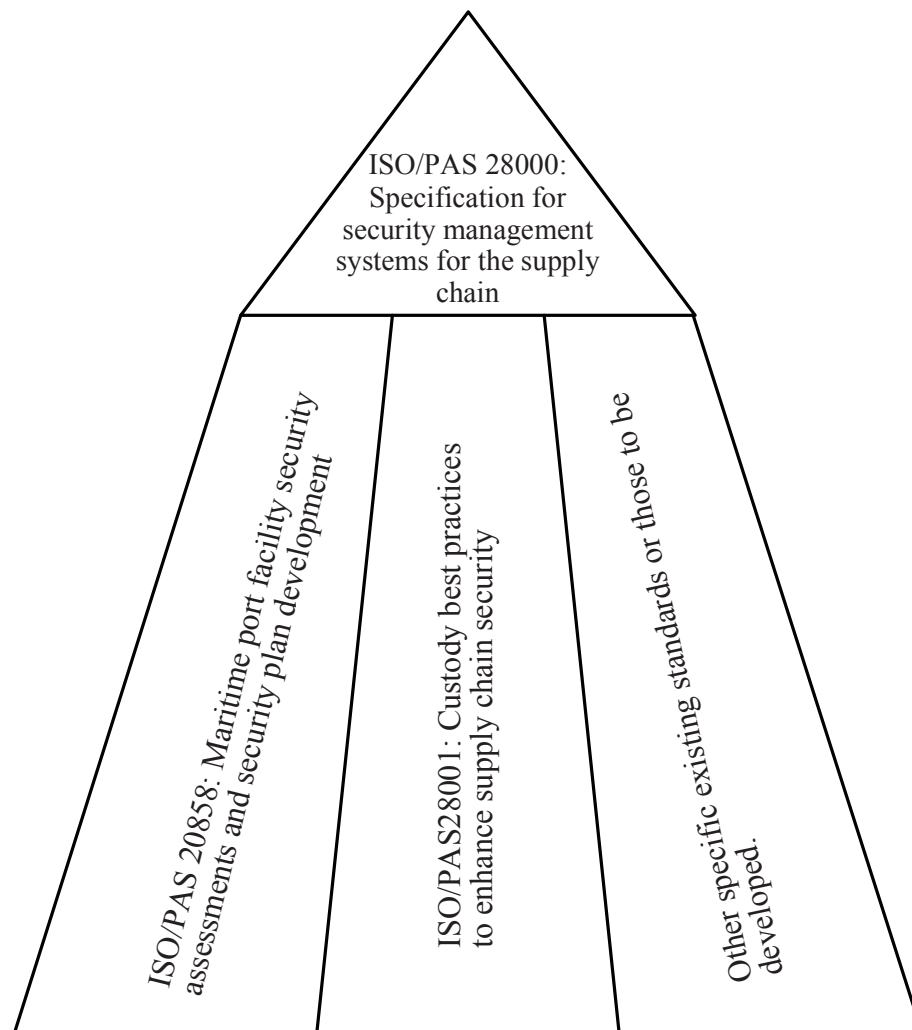


Figure 1 — Relationship between ISO/PAS 28000 and other relevant standards

This Publicly Available Specification is intended to apply in cases where an organization's supply chains are required to be managed in a secure manner. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

Compliance with a Publicly Available Specification does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system to this Publicly Available Specification may be verified by an external or internal auditing process.

This Publicly Available Specification is based on the ISO format adopted by ISO 14001:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this Publicly Available Specification. It is not the intention of this Publicly Available Specification to duplicate governmental requirements and standards regarding supply chain security management to which the organization has already been certified or verified compliant. Verification may be by an acceptable first, second, or third party organization.

NOTE This Publicly Available Specification is based on the methodology known as Plan-Do-Check-Act (PDCA). PDCA can be described as follows.

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy.
- Do: implement the processes.
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.
- Act: take actions to continually improve performance of the security management system.