

This is a preview of "ISO 28000:2007". [Click here to purchase the full version from the ANSI store.](#)

First edition  
2007-09-15

---

---

## 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 28000:2007(E)

© ISO 2007

This is a preview of "ISO 28000:2007". [Click here to purchase the full version from the ANSI store.](#)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2007

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO 28000:2007". [Click here to purchase the full version from the ANSI store.](#)

## 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 28000:2007, ISO 14001:2004 and ISO 9001:2000.....	13
Bibliography .....	16

This is a preview of "ISO 28000:2007". [Click here to purchase the full version from the ANSI store.](#)

## 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 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.

This first edition of ISO 28000 cancels and replaces ISO/PAS 28000:2005, which has been technically revised

This is a preview of "ISO 28000:2007". [Click here to purchase the full version from the ANSI store.](#)

## Introduction

This International Standard 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. It 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.

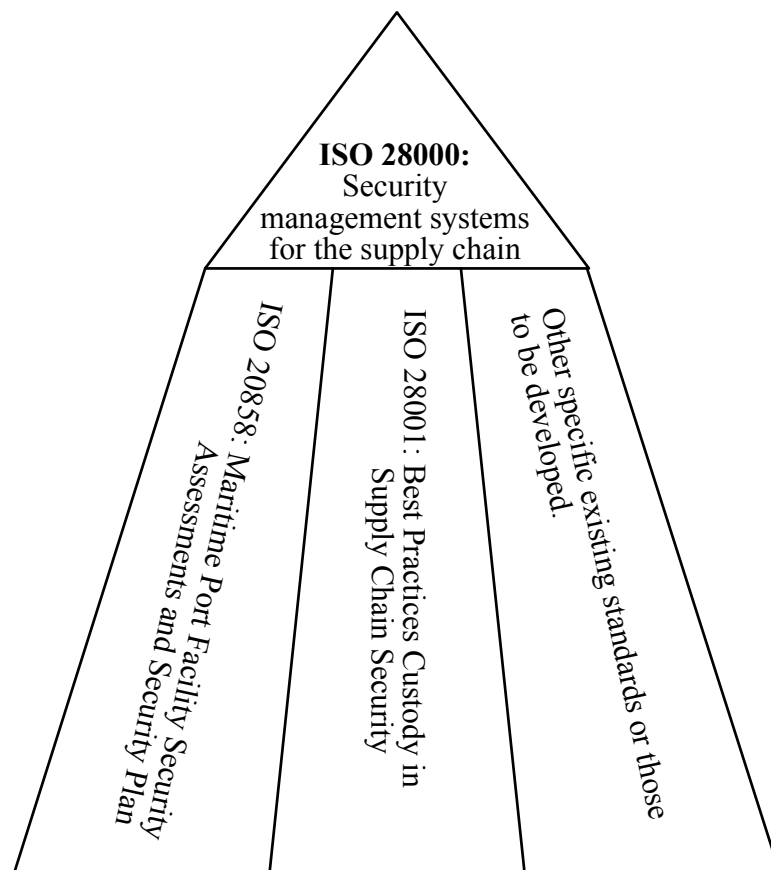


Figure 1 — Relationship between ISO 28000 and other relevant standards

This is a preview of "ISO 28000:2007". [Click here to purchase the full version from the ANSI store.](#)

This International Standard 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 an International Standard does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system with this International Standard may be verified by an external or internal auditing process.

This International Standard 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 International Standard. It is not the intention of this International Standard 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 International Standard 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.