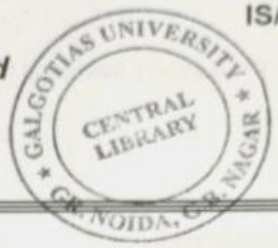
IS-0031

भारतीय मानक
Indian Standard

IS/ISO 28004-4 : 2014
(Reaffirmed 2020)



आपूर्ति श्रृंखला के लिए सुरक्षा प्रबंधन प्रणाली — आई एस ओ 28000 के कार्यान्वयन के लिए दिशानिर्देश

भाग 4 आई एस ओ 28000 के अनुपालन पर अतिरिक्त विशिष्ट मार्गदर्शन यदि आई एस ओ 28001 अनुपालन एक प्रबंधन उद्देश्य है

Security Management Systems for the Supply Chain — Guidelines for the implementation of ISO 28000

Part 4 Additional Specific Guidance on Implementing ISO 28000 if Compliance with ISO 28001 is a Management Objective

ICS 47.020.99

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.gov.in www.standardsbis.in

January 2020

Price Group 3

Management and Productivity Sectional Committee, MSD 04

NATIONAL FOREWORD

This Indian Standard (Part 4) which is identical with ISO 28004-4 : 2014 'Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective 'issued by the International Organization for Standardization (ISO) was be adopted by the Bureau of Indian Standards on recommendation of the Management and Productivity Sectional Committee and approval of the Management and Systems Division Council.

The text of ISO Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain terminologies and conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker, while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to certain International Standards for which Indian Standards also exist. The corresponding Indian Standards, which are to be substituted in their respective places, are listed below along with their degree of equivalence for the editions indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 28000: 2007 Specification for security management systems for the supply chain	IS/ISO 28000 : 2007 Specification for security management systems for the supply chain	Identical
ISO 28001 : 2007 Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance	IS/ISO 28001 : 2007 Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance	Identical with ISO 28001 : 2007
ISO 28004-1: 2007 Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles	IS/ISO 28004-1 : 2007 Security management systems for the supply chain — Guidelines for the implementation of ISO 28000: Part 1 General principles	Identical with ISO 28004- 1 : 2007

The technical committee has reviewed the provisions of the following International Standard referred in this adopted standard and has decided that it is acceptable for use in conjunction with this standard:

International Standard	*Title*
ISO 20858	Ships and marine technology — Maritime port facility security assessments and security plan development

Contents

Page

Introduction

This part of ISO 28004 has been developed to supplement ISO 28004-1. The additional guidance in this part of ISO 28004, while amplifying the general guidance provided in the main body of ISO 28004-1, does not conflict with the general guidance. While ISO 28000 is less specific than ISO 28001 on certain technical security requirements, they do not conflict. This part of ISO 28004 helps to meet the Authorized Economic Operator security criteria.

Indian Standard

SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN — GUIDELINES FOR THE IMPLEMENTATION OF ISO 28000

PART 4 ADDITIONAL SPECIFIC GUIDANCE ON IMPLEMENTING ISO 28000 IF COMPLIANCE WITH ISO 28001 IS A MANAGEMENT OBJECTIVE

1 Scope

This part of ISO 28004 provides additional guidance for organizations adopting ISO 28000 that also wish to incorporate the Best Practices identified in ISO 28001 as a management objective on their international supply chains. The Best Practices in ISO 28001 both help organizations establish and document levels of security within an international supply chain and facilitate validation in national Authorized Economic Operator (AEO) programmes that are designed in accordance with the World Customs Organization (WCO) Framework of Standards.

This part of ISO 28004 is not designed as a standalone document. The main body of ISO 28004-1 provides significant guidance pertaining to required inputs, processes, outputs and other elements required by ISO 28000. This part of ISO 28004 provides additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective.

Some requirements specified in the WCO AEO programme are government functions and are not addressed in the ISO international standards. These include:

— Demonstrated Compliance with Customs Requirements. Customs are to take into account the demonstrated compliance history of a prospective AEO when considering the request for AEO status.

— Satisfactory System for Management of Commercial Records. The AEO is to maintain timely, accurate, complete and verifiable records relating to import and export. Maintenance of verifiable commercial records is an essential element in the security of the international trade supply chain.

— Financial Viability. Financial viability of the AEO is an important indicator of an ability to maintain and improve upon measures to secure the supply chain.

— Consultation, Co-operation and Communication. Customs, other competent authorities and the AEO at all levels — international, national and local — should consult regularly on matters of mutual interest, including supply chain security and facilitation measures, in a manner which will not jeopardize enforcement activities. The results of this consultation should contribute to Customs development and maintenance of its risk management strategy.

2 Normative references

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

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

ISO 28000, *Specification for security management systems for the supply chain*

ISO 28001, *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance*

ISO 28004-1, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles*

3 General information

The diagram in Figure 1 provides an illustration of how compliance and possible certification to ISO 28000 incorporating the best practices of ISO 28001 complements the requirements of national, regional or economic Authorized Economic Operator programs and as well as those of certain industry programs and facilitates the validations of such programs. Organizations may also choose to adopt ISO 28000 and ISO 28001 to improve and document supply chain security management without the goal of achieving AEO certification.

Figure 1 — Complementary security standards to secure supply chain

4 Organization of this part of ISO 28004

Clause 5 provides a series of charts showing the synergy between the World Customs Organization SAFE Framework Authorized Economic Operator requirements and the clauses in ISO 28000 and ISO 28001 that address the AEO requirements.

Clause 6 provides practical guidance as to where the various requirements of ISO 28001 would plug into ISO 28000 as inputs, processes or outputs.

Clause 7 provides notes, to clarify slight differences in terminology used in ISO 28000 and ISO 28001.

5 Synergy between the World Customs Organization SAFE Framework Authorized Economic Operator requirements

In Tables 1 to 9 that follow, the AEO requirement sections are listed first in **Bold** type. This is followed by a brief summary of that requirement. In the boxes below each summary are the clauses of ISO 28000 and ISO 28001 that address those requirements. The majority of the WCO AEO requirements are addressed in Tables 1 to 9 and those defined as government functions in the introduction section of this part of ISO 28004. Please note that National AEO programs may have additional requirements such as specific minimum criteria that may not be fully addressed in ISO 28000 or ISO 28001.

Table 1

A. Education, Training and Awareness
Customs and AEOs shall develop mechanisms for the education and training of personnel regarding security policies, recognition of deviations from those policies and understanding what actions must be taken in response to security lapses
ISO 28000, 4.4.2 (Competence, training and awareness) ISO 28001, 5.3.1 (Assessment personnel)

Table 2

B. Information Exchange, Access and Confidentiality
Customs and AEOs, as part of an overall comprehensive strategy to secure sensitive information, shall develop or enhance the means by which entrusted information is protected against misuse and unauthorized alteration.
ISO 28000, 4.2 (Security management policy), 4.4.5 (Document and data control), 4.5.4 (Controls of Records) ISO 28001, 5.8 (Protection of the security information)

Table 3

C. Cargo Security
Customs and AEOs shall establish and/or bolster measures to ensure that the integrity of cargo is maintained and that access controls are at the highest appropriate level, as well as establishing routine procedures that contribute to the security of cargo.
ISO 28000, 4.4.6 (Operational control) ISO 28001, 5.4 (Development of the supply chain security plan)

Table 4

D. Conveyance Security
Customs and AEOs shall jointly work toward the establishment of effective control regimes, where not already provided for by other national or international regulatory mandate, to ensure that transport conveyances are capable of being effectively secured and maintained
ISO 28000, 4.4.6 (Operational control) ISO 28001, 5.4 (Development of the supply chain security plan)

Table 5

E. Premises Security
Customs, after taking into account the views of AEOs and their necessary compliance with mandatory international standards, shall establish the requirements for the implementation of meaningful Customs-specific security enhancement protocols that secure buildings, as well as ensure the monitoring and controlling of exterior and interior perimeters.
ISO 28000, 4.4.6 (Operational control) ISO 28001, 5.4 (Development of the supply chain security plan)

Table 6

F. Personnel Security
Customs and AEOs shall, based on their authorities and competencies, screen the background of prospective employees to the extent legally possible. In addition, they shall prohibit unauthorized access to facilities, transport conveyances, loading docks and cargo areas that may reasonably affect the security of those areas in the supply chain under their responsibility
ISO 28000, 4.4.6 (Operational control) ISO 28001, 5.4 (Development of the supply chain security plan)

Table 7

G. Trading Partner Security
Customs shall establish AEO requirements and mechanisms whereby the security of the global supply chain can be bolstered through the commitment of trading partners to voluntarily increase their security measures.
ISO 28000, 4.4.6 (Operational control) ISO 28001, 4.1 (Statement of application), 4.2 (Business partners), 4.3 (Internationally accepted certificates or approvals), 4.4 (Business partners exempt from security declaration requirement), 4.5 (Field of Application)

Table 8

H. Crisis Management and Incident Recovery
In order to minimize the impact of a disaster or terrorist incident, crisis management and recovery procedures should include advance planning and establishment of processes to operate in such extraordinary circumstances.
ISO 28000, 4.5.3 (Security-related failures, incidents, non-conformances and corrective and preventive action), 4.4.6 (Operational control), 4.4.7 (Emergency preparedness, response and security recovery) ISO 28001, 5.7 (Actions required after a security incident)

Table 9

I. Measurement, Analyses and Improvement
The AEO and Customs should plan and implement monitoring, measurement, analysis and improvement processes in order to: — assess consistency with these guidelines; — ensure integrity and adequacy of the security management system; — identify potential areas for improving the security management system in order to enhance supply chain security.
ISO 28000, 4.1 (General requirements), 4.3 (Security risk assessment and planning) ISO 28001, 5.1 (Supply chain security process- General) 5.2 (Identification of the scope of security assessment), 5.3.2 (Assessment process), 5.4 (Development of the supply chain security plan), 5.5 (Execution of the supply chain security plan), 5.6 (Documentation and monitoring of the supply chain security process)

6 Practical guidance as to where the various requirements of ISO 28001 would plug into ISO 28000 as inputs, processes or outputs

ISO 28000	Best Practices Additions from ISO 28001	Comments
4.2 Security Policy	A policy statement that specifies where the Best Practices will be applied. This information can be drawn from the documentation of the information required in ISO 28001, 4.1 a and b	Organizations that are adopting the Best Practices for the purposes of ultimately being validated as a Authorized Economic Operator (AEO) should confer with the Customs Administration(s) with authority to confer AEO status to ensure that the intended scope of the Best Practices application is adequate to gain AEO status by that Customs Administration.
4.3.1 Security Risk Assessment	Clause 5.3.1 specifies the skills and knowledge of the personnel that will conduct the security assessment Clause 5.3.2 requires the inclusion of security threat scenarios deemed necessary by appropriate government officials in addition to those proposed by the assessment personnel. Documentation required is: a) All security threat scenarios considered b) Processes used in the evaluating those threats; and c) All countermeasures identified and prioritized	ISO 28001 does not require organizations in the supply chain that hold Internationally accepted certificates or approvals (as defined in 4.3), nor does it require organizations that have been certified compliant with a management standard integrating either ISO 20858 or ISO 28001 to redo security assessments on those portions of the supply chain already assessed (see 4.4). Note: If AEO validation or certification is sought, the relevant Customs administration or the certifying body, involved, shall determine the selection of International Certificates or approvals, and certifications, that are recognized. ISO 28001, Clause 4.2 recognizes that some business partners in the supply chain will not wish to participate in a security assessment for each company they deal with. In these cases ISO 28001 allows these companies to state in writing the security measures that they will be providing (declarations of security). The credibility of these declarations must be reviewed as specified in 4.5.
4.3.1 Security Risk Planning	Clause 5.4 specifies the requirements of the security plan developed for the covered sections of the supply chain(s). Organizations are required to review and consider for use the guidance in informative Annexes A and B when developing their security plans.	
		ISO 28001, Clauses 5.5 to 5.6.2 require the security plan developed be implemented and monitored as part of a management system
4.5.3 Security-related failures, incidents, non-conformances and corrective and preventative action.	Clause 5.7 in addition requires that in the event of a security breach, the organization shall follow reporting procedures to Customs and/or appropriate law enforcement agencies.	

7 Notes on terminology

Some small terminology differences exist between ISO 28000 and ISO 28001. In addition some amplifying information concerning the linkage of certain terms used in the international standards was found to be needed. This clause provides the amplifying information to address these needs.

Terminology from ISO 28000 and ISO 28004	Terminology from ISO 28001	Comments
Facility, Clause 3.1	Asset, Clause 3.2	The intent and definitions of these two terms are synonymous in ISO 28000 and ISO 28001
Security Management Programme, Clause 3.6		This is an element of a management system. The security programme outlined in ISO 28001 may be considered one such programme.
Stakeholder, Clause 3.8	Business Partner, Clause 3.4	Stakeholder is defined in ISO 28000 and includes a broad number of entities with vested interests in the performance of the Security Management system. Business Partner is defined in ISO 28001 as those entities in the supply chain in which a business relationship exists. Business partners can be thought of as a subset of the larger stakeholder set.
	Organization in the supply chain, Clause 3.15	Stakeholder is defined in ISO 28000 and is used to describe organizations in the supply chain that produce, handle, transport, or process goods or related information in the supply chain that is adopting ISO 28001.
	International supply chain, Clause 3.12	ISO 28001 defines this term as a supply chain that at some point crosses an international or economic border. Since not all supply chains cross such a border an international supply chain can be considered a further subset of the larger ISO 28000 supply chain definition.
Risk, Clause 3.10	Security Incident Scoring, (Clause B.5-Step four)	While the terms 'Risk' is not defined in ISO 28001 it is clearly described as a factor of likelihood and consequences in several sections of ISO 28001 where security incident scoring and the development of countermeasures are described.
Threat, Clause 3.3	Security Threat Scenario, Clause 3.27 Security Incident, Clause 3.21 Consequence, Clause 3.6 Target, Clause 3.26	While ISO 28000 defines 'Threat' as any possible action or series of actions with damaging potential to any of the stakeholders...." The word criminal can be implied in front of the word action since the management system is security related. ISO 28001 simply breaks the term threat into four parts (Clauses 3.27, 3.21, 3.26 and 3.6) that collectively define a potential threat scenario and target that could lead to a security incident with consequences.
	Scope of service, Clause 3.17 (is an element in the Statement of application - 4.1)	ISO 28001 defines this term as function(s) that an organization in the supply chain performs, and where it performs this/these functions. This concept is contained in discussions in ISO 28004-1 that refer to defining boundaries and scope of the management system.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: MSD 04 (13343).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices: *Telephones*

Central : Manak Bhavan, 9 Bahadur Shah Zafar Marg, NEW DELHI 110002 — 2323 7617, 2323 3841

Eastern : 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi, KOLKATA 700054 — 2337 8499, 2337 8561, 2337 8626, 2337 9120

Northern : Plot No. 4-A, Sector 27-B, Madhya Marg, CHANDIGARH 160019 — 265 0206, 265 0290

Southern : C.I.T. Campus, IV Cross Road, CHENNAI 600113 — 2254 1216, 2254 1442, 2254 2519, 2254 2315

Western : Manakalaya, E9 MIDC, Marol, Andheri (East), MUMBAI 400093 — 2832 9295, 2832 7858, 2832 7891, 2832 7892

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. DURGAPUR. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. JAMMU. JAMSHEDPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAIPUR. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi