

INTERNATIONAL STANDARD

ISO
28000

Second edition
2022-03

Security and resilience — Security management systems — Requirements



Reference number
ISO 28000:2022(E)

CISO 2022



COPYRIGHT PROTECTED DOCUMENT

C ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office

CP 401 · Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 0111

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	V
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	4
4.1 Understanding the organization and its context	4
4.2 Understanding the needs and expectations of interested parties	4
4.2.1 General	4
4.2.2 Legal, regulatory and other requirements	4
4.2.3 Principles	5
4.3 Determining the scope of the security management system	6
4.4 Security management system	6
5 Leadership	7
5.1 Leadership and commitment	7
5.2 Security policy	7
5.2.1 Establishing the security policy	7
5.2.2 Security policy requirements	8
5.3 Roles, responsibilities and authorities	8
6 Planning	8
6.1 Actions to address risks and opportunities	8
6.1.1 General	8
6.1.2 Determining security-related risks and identifying opportunities	9
6.1.3 Addressing security-related risks and exploiting opportunities	9
6.2 Security objectives and planning to achieve them	9
6.2.1 Establishing security objectives	9
6.2.2 Determining security objectives	10
6.3 Planning of changes	10
7 Support	10
7.1 Resources	10
7.2 Competence	10
7.3 Awareness	11
7.4 Communication	1
7.5 Documented information	11
7.5.1 General	11
7.5.2 Creating and updating documented information	11
7.5.3 Control of documented information	12
8 Operation	12
8.1 Operational planning and control	12
8.2 Identification of processes and activities	12
8.3 Risk assessment and treatment	13
8.4 Controls	13
8.5 Security strategies, procedures, processes and treatments	14
8.5.1 Identification and selection of strategies and treatments	14
8.5.2 Resource requirements	14
8.5.3 Implementation of treatments	14
8.6 Security plans	14
8.6.1 General	14
8.6.2 Response structure	14
8.6.3 Warning and communication	15
8.6.4 Content of the security plan	15

8.6.5 Recovery 16

9 Performance evaluation 16

9.1 Monitoring , measurement , analysis and evaluation 16

9.2 Internal audit 17

9.2.1 General 17

9.2.2 Internal audit programme 17

9.3 Management review 17

9.3.1 General 17

9.3.2 Management review inputs 18

9.3.3 Management review results 18

10 Improvemen 18

10.1 Continual improvemen 18

10.2 Nonconformity and corrective action 19

Bibliography 20

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, Security and resilience.

This second edition cancels and replaces the first edition (ISO 28000:2007), which has been technically revised, but maintains existing requirements to provide continuity for organizations using the previous edition. The main changes are as follows:

- recommendations on principles have been added in [Clause 4](#) to give better coordination with ISO 31000;
- recommendations have been added in [Clause 8](#) for better consistency with ISO 22301, facilitating integration including:
 - security strategies, procedures, processes and treatments;
 - security plans.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Most organizations are experiencing an increasing uncertainty and volatility in the security environment. As a consequence, they face security issues that impact on their objectives, which they want to address systematically within their management system. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

This document specifies requirements for a security management system, including those aspects critical to the security assurance of the supply chain. It requires the organization to:

- assess the security environment in which it operates including its supply chain (including dependencies and interdependencies);
- determine if adequate security measures are in place to effectively manage security-related risks;
- manage compliance with statutory, regulatory and voluntary obligations to which the organization subscribes;
- align security processes and controls, including the relevant upstream and downstream processes and controls of the supply chain to meet the organization's objectives.

Security management is linked to many aspects of business management. They include all activities controlled or influenced by organizations, including but not limited to those that impact on the supply chain. All activities, functions and operations should be considered that have an impact on the security management of the organization including (but not limited to) its supply chain.

With regard to the supply chain, it has to be considered that supply chains are dynamic in nature. Therefore, some organizations managing multiple supply chains may look to their providers to meet related security standards as a condition of being included in that supply chain in order to meet requirements for security management.

This document applies the Plan-Do-Check-Act (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's security management system, see [Table 1](#) and [Figure 1](#).

Table 1—Explanation of the PDCA model

Plan (Establish)	Establish security policy, objectives, targets, controls, processes and procedures relevant to improving security in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the security policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against security policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the security management system by taking corrective action, based on the results of management review and reappraising the scope of the security management system and security policy and objectives.

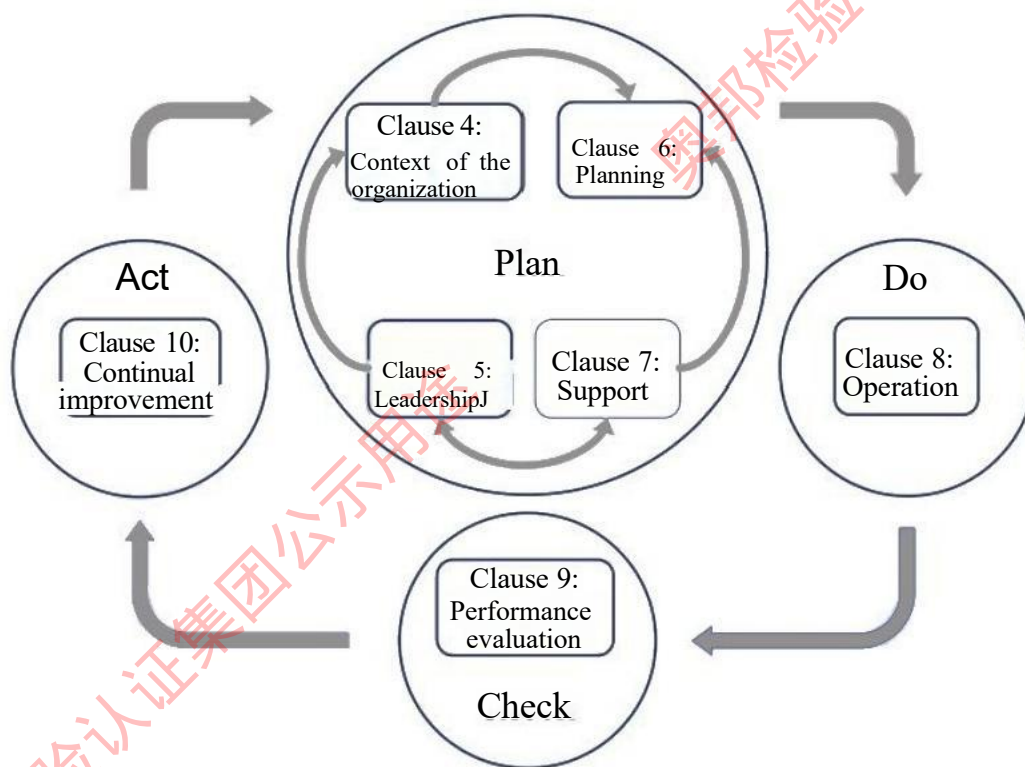


Figure 1—PDCA model applied to the security management system

This ensures a degree of consistency with other management system standards, such as ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001, etc., thereby supporting consistent and integrated implementation and operation with related management systems.

For organizations that so wish, conformity of the security management system to this document may be verified by an external or internal auditing process.

Security and resilience—Security management systems — Requirements

1 Scope

This document specifies requirements for a security management system, including aspects relevant to the supply chain.

This document is applicable to all types and sizes of organizations (e.g. commercial enterprises, government or other public agencies and non-profit organizations) which intend to establish, implement, maintain and improve a security management system. It provides a holistic and common approach and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, internal or external, at all levels.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 22300, Security and resilience—Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at <https://www.iso.org/obp>

— IEC Electropedia: available at <https://www.electropedia.org/>

3.1

organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.2)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the security management system (3.5).

3.2

interested party (preferred term)

stakeholder (admitted term)

person or organization (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

国际标准

ISO
28000

第二版
2022-03

安全与韧性 安全管理体系 要求



参考编号 ISO
28000:2022(E)

© ISO 2022

奥邦检验认证集团

奥邦检验认证集团公示用途

奥邦检验认证集团公示用途



受版权保护的文件

© ISO 2022

保留所有权利。除非另有规定，或在实施过程中需要，未经事先书面许可，不得以任何形式或任何手段，包括电子或机械，复制或利用本出版物的任何部分，或在互联网或内部网上发布。可以通过以下地址向国际标准化组织或请求者所在国家的国际标准化组织的成员机构申请许可。

ISO版权局
CP 401 - Ch. de Blandonnet 8
CH-1214 Vernier, Geneva 电话: +41 22 749 01 11
电子邮件: copyright@iso.org
网站: www.iso.org

发表于瑞士

内容

前言 简介

1 范围

2 规范性参考资料

3 术语和定义

4 组织的背景

4.1 了解组织和其背景

4.2 了解有关各方的需求和期望

4.2.1 一般

4.2.2 法律、监管和其他要求

4.2.3 原则

4.3 确定安全管理体系的范围

4.4 安全管理制度

5 领导人

5.1 领导和承诺

5.2 安全政策

5.2.1 建立安全政策

5.2.2 安全政策要求

5.3 角色、责任和权力

6 规划

6.1 应对风险和机遇的行动

6.1.1 一般

6.1.2 确定与安全有关的风险并确定机会

6.1.3 应对与安全有关的风险和利用机会

6.2 安全目标和实现这些目标的规划

6.2.1 确立安全目标

6.2.2 确定安全目标

6.3 变化的规划

7 支持

7.1 资源

7.2 能力

7.3 认识

7.4 沟通

7.5 记录的信息

7.5.1 一般

7.5.2 创建和更新文件化的信息

7.5.3 对文件资料的控制

8 运作

8.1 业务规划和控制

8.2 确定过程和活动

8.3 风险评估和治疗

8.4 控制措施

8.5 安全战略、程序、过程和处理

8.5.1 确定和选择战略和治疗方法

8.5.2 所需资源

8.5.3 实施治疗

8.6 安全计划

8.6.1 一般

8.6.2 响应结构

8.6.3 警告和沟通

8.6.4 安全计划的内容

	8.6.5	恢复
9		业绩评估
	9.1	监测、测量、分析和评价
	9.2	内部审计
	9.2.1	一般
	9.2.2	内部审计方案
	9.3	管理审查
	9.3.1	一般
	9.3.2	管理审查投入
	9.3.3	管理审查结果
10		改进
	10.1	持续改进
	10.2	不合格品和纠正措施

前言

ISO（国际标准化组织）是一个由国家标准机构（ISO成员机构）组成的全球联合会。制定国际标准的工作通常是通过ISO技术委员会进行的。每个对某一主题感兴趣的成员机构都有权在该技术委员会中任职。与国际标准化组织联络的国际组织、政府和非政府组织也参与这项工作。国际标准化组织与国际电工委员会（IEC）在所有电工标准化问题上紧密合作。

用于制定本文件的程序和打算进一步维护本文件的程序在ISO/IEC指令第1部分中有描述。特别要注意的是，不同类型的ISO文件需要不同的批准标准。本文件是根据ISO/IEC指令第2部分的编辑规则起草的（见www.iso.org/directives）。

请注意，本文件中的某些内容可能是专利权的对象。ISO不负责识别任何或所有此类专利权。在文件制定过程中发现的任何专利权的细节将在导言中和/或在ISO收到的专利声明列表中（见www.iso.org/patents）。

本文件中使用的任何商品名称是为方便用户而提供的信息，不构成对其的认可。

关于标准的自愿性质的解释，与合格评定有关的ISO特定术语和表达方式的含义，以及关于ISO在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，见www.iso.org/iso/foreword.html。

本文件由ISO/TC 292技术委员会（安全和复原力）编写。

第二版取消并取代了第一版（ISO 28000:2007），第一版在技术上进行了修订，但保留了现有的要求，为使用前一版的组织提供连续性。主要变化如下。

- 在[第4条中](#)加入了关于原则的建议，以便与ISO 31000更好地协调。
- 在[第8条中](#)增加了建议，以便与ISO 22301更好地保持一致，促进整合，包括。
 - 安全战略、程序、过程和处理。
 - 安全计划。

对本文件的任何反馈或问题应直接向用户的国家标准机构提出。这些机构的完整名单可在www.iso.org/members.html。

简介

大多数组织正经历着安全环境中越来越多的不确定性和波动性。因此，他们面临着影响其目标的安全问题，他们希望在其管理系统中系统地解决这些问题。正式的安全管理方法可以直接促进组织的业务能力和可信度。

本文件规定了对安全管理系统的要求，包括对供应链安全保障至关重要的那些方面。它要求组织做到

- 评估其运作的安全环境，包括其供应链（包括依赖性和相互依赖性）。
- 确定是否有足够的安全措施来有效管理与安全有关的风险。
- 管理对组织所认同的法定、监管和自愿义务的遵守情况。
- 调整安全流程和控制，包括供应链的相关上游和下游流程和控制，以满足组织的目标。

安全管理与企业管理的许多方面相关联。它们包括由组织控制或影响的所有活动，包括但不限于对供应链有影响的活动。应考虑对组织的安全管理有影响的所有活动、功能和操作，包括（但不限于）其供应链。

关于供应链，必须考虑到供应链在本质上是动态的。因此，一些管理多个供应链的组织可能希望其供应商达到相关的安全标准，作为被纳入该供应链的一个条件，以满足安全管理的要求。

本文件将计划-执行-检查-行动（PDCA）模式应用于组织的安全管理系统的规划、建立、实施、运行、监控、审查、维护和持续改进其有效性，[见表1](#)和[图1](#)。

表1--PDCA模型的解释

计划(建立)	建立与改善安全有关的安全政策、目标、指标、控制、流程和程序，以提供与组织的总体政策和目标相一致的结果。
做 (实施和操作)	实施和操作安全政策、控制、程序和程序。
检查 (监测和审查)	根据安全政策和目标监测和审查业绩，将结果报告给管理层进行审查，并确定和授权采取补救和改进行动。
诉讼 (保持和改善)	根据管理审查的结果，采取纠正措施，维护和改进安全管理系统，重新评估安全管理系统的范围和安全政策及目标。

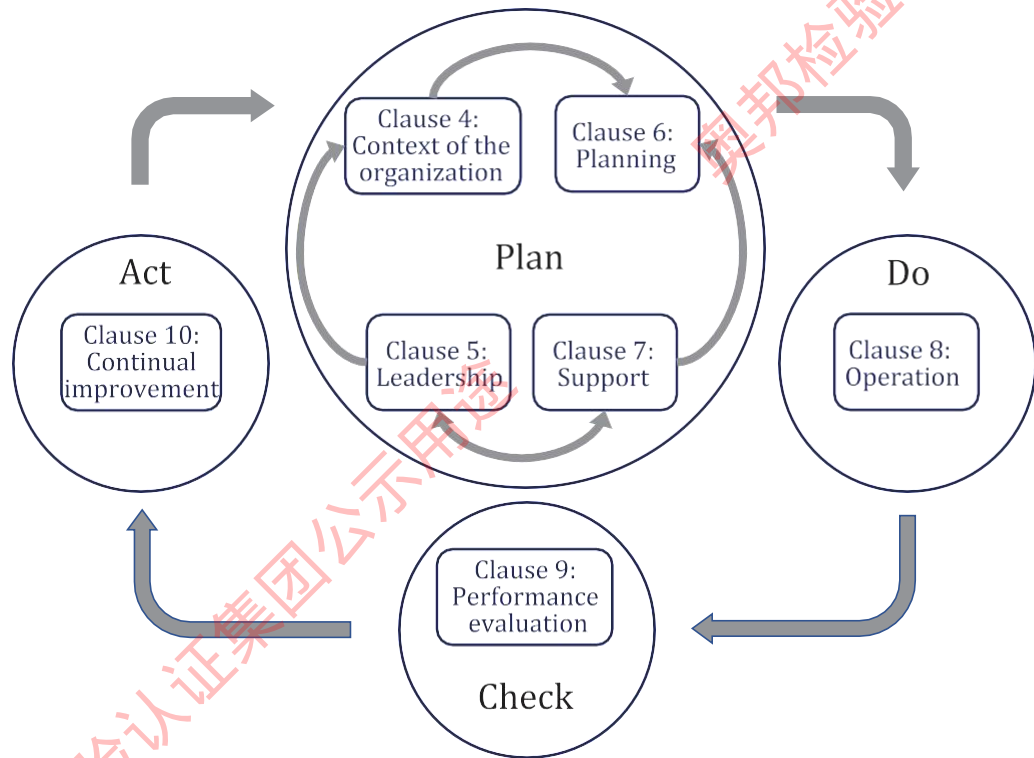


图1 - PDCA模型应用于安全管理系统

这确保了与其他管理体系标准，如ISO 9001、ISO 14001、ISO 22301、ISO/IEC 27001、ISO 45001等的一定程度的一致性，从而支持与相关管理体系的一致和综合实施和运行。

对于有此愿望的组织，可以通过外部或内部审计程序来验证安全管理系统与本文件的一致性。

安全与韧性 安全管理体系 要求

1 范围

本文件规定了安全管理体系的要求，包括与供应链相关的方面。

本文件适用于所有类型和规模的组织（如商业企业、政府或其他公共机构和非营利组织），它们打算建立、实施、维护和改进安全管理体系。它提供了一个整体的、共同的方法，并不针对具体行业或部门。

这份文件可以在组织的整个生命周期中使用，并且可以适用于任何活动，无论是内部的还是外部的，各级的。

2 规范性参考资料

以下文件在文中被提及，其部分或全部内容构成本文件的要求。对于注明日期的参考文献，仅适用于所引用的版本。对于未注明日期的参考文件，适用于所参考文件的最新版本（包括任何修正案）。

ISO 22300，*安全和复原力- 词汇表*

3 术语和定义

在本文件中，适用ISO 22300和下列术语和定义。国际标准化组织和国际电工委员会在以下地址维护用于标准化的术语数据库。

— ISO在线浏览平台：可在<https://www.iso.org/obp>

— IEC Electropedia：可在<https://www.electropedia.org/>

3.1

组织

有自己的职能、责任、权力和关系以实现其目标的人或团体（3.7）。

条目注1。组织的概念包括但不限于独资企业、公司、企业、公司、企业、当局、合伙企业、慈善机构或其部分或组合，无论是否成立、公共或私人。

条目注释2。如果该组织是一个较大实体的一部分，“组织”一词仅指该较大实体中属于安全管理体系（3.5）范围的部分。

3.2

利害关系人

利益相关者

能影响、受影响或认为自己受某一决定或活动影响的人或组织（3.1）。

3.3 最高管理层

最高层指挥和控制组织的人或团体 (3.1)。

条目注释1。最高管理层有权在组织内下放权力和提供资源。

条目注释2。如果管理体系的范围 (3.4) 只包括一个组织的一部分，那么最高管理层是指指导和控制该部分组织的人。

3.4 管理系统

一套相互关联或相互作用的组织要素 (3.1)，以建立政策 (3.6) 和目标 (3.7)，以及实现这些目标的过程 (3.9)。

条目注释1。一个管理系统可以解决单一学科或几个学科的问题。

条目注释2。管理体系要素包括组织的结构、角色和责任、规划和运行。

3.5 安全管理系统

由协调的政策 (3.6)、程序 (3.9) 和实践组成的系统，一个组织通过它来管理其安全目标 (3.7)。

3.6 政策

一个组织的意图和方向 (3.1)，由其最高管理层正式表达 (3.3)。

3.7 目标 要实现的结果

条目注释1。一个目标可以是战略的、战术的、或行动的。

条目注释2。目标可以与不同的学科有关（如财务、健康和环境以及安全）。例如，它们可以是整个组织的，也可以是针对某个项目、产品和过程的 (3.9)。

条目注3。目标可以用其他方式表达，例如，作为预期的结果，作为目的，作为操作标准，作为安全目标，或通过使用具有类似含义的其他词汇（例如，目的，目标，或目标）。

条目注释4。在安全管理系统方面 (3.5)，安全目标是由组织制定的 (3.1)，与安全策略 (3.6) 一致，以实现具体的结果。

3.8 风险

不确定性对目标的影响 (3.7)

条目注1。效果是对预期的偏离。它可以是积极的、消极的或两者兼而有之，并且可以解决、创造或导致机会和威胁。

条目注释2。目标可以有不同的方面和类别，也可以在不同的层面上应用。

条目注释3。风险通常用风险源、潜在事件、其后果和其可能性来表示。

3.9 过程

一组相互关联或相互作用的活动，使用或改变输入以提供一个结果。

条目注释1。一个过程的结果是否被称为产出、产品或服务，取决于背景。的参考。

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1) 通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2) 也可通过客服电话咨询 **025-85307007**。