安全与韧性-安全管理体系-要求
ISO 28000：2022

发布单位：国际标准化组织

浙江公信认证有限公司
（仅供内部交流使用）

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。

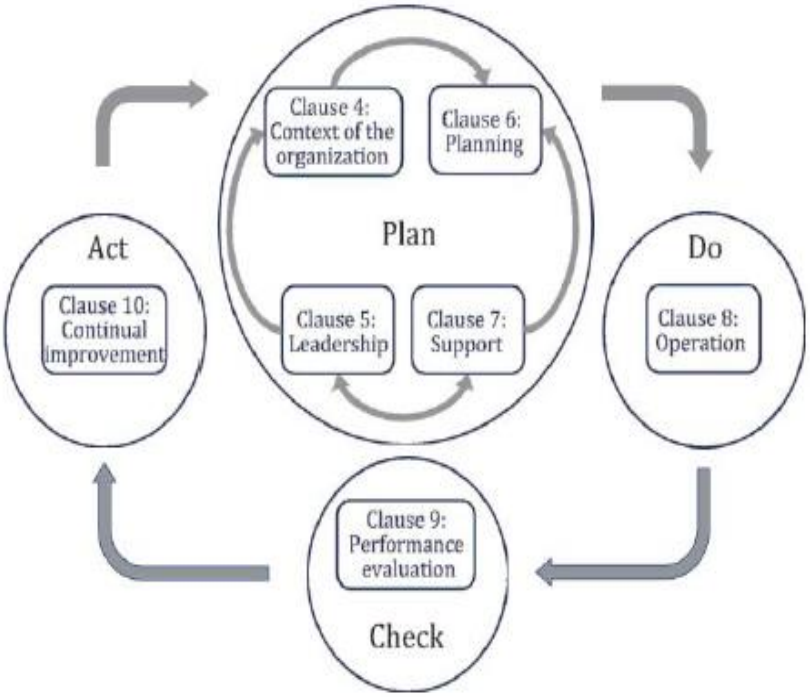

图1 - P DCA模型应用于安全管理系统

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）建立、实施、维护和改进安全管理体系。本文件提供了一个整体的、共同的方法，并不针对具体行业或部门。

本文件适用于在组织的整个生命周期以及各个层级内部、外部的活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO 22300　安全与韧性　术语

3 术语和定义

ISO 22300 界定的以及下列术语和定义适用于本文件。

ISO 和 IEC 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

为实现目标，具有自身职能、责任、权限和关系的个人或群体。

注 1：组织的概念包括但不限于个体经营户、公司、企业、商行、机构、合伙企业、慈善组织或机构，或其组成部分或组合形式，无论是否已注册、属于公营还是私营性质。

注 2：如果该组织是一个较大实体的一部分，则“组织”一词仅指该较大实体中属于安全管理体系范围的部分。

3.2 利益相关方(首选术语)/利益相关者(许用术语)

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。

3.3 最高管理者

在最高层指挥并控制组织的一个人或一组人。

注 1：最高管理者有权在组织内部授权并提供资源。

如有需要，请通过如下方式联系本机构索取相关认证依据（标准）全文。

电话：0571-85067843

邮箱：wangxin@gac.org.cn