国际标准

ISO 28000

第二版
2022-03

安全和韧性 安全管理体系 要求

参考编号 ISO
28000:2022(E)

受版权保护的文件

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

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。

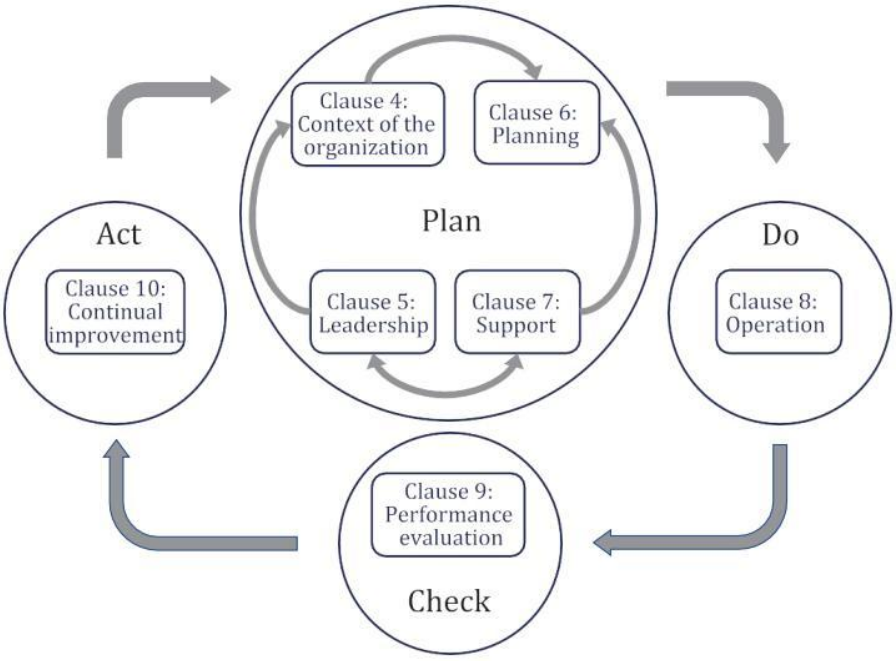

图1 - P DCA模型应用于安全管理系统

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。

安全和复原力 - 安全管理系统 - 要求

1 范围

本文件规定了安全管理系统的要求，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系统。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*安全管理系统*（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、健康和安全以及环境）。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。

3.10
能力
运用知识和技能来实现预期结果的能力

3.11
记载的信息
一个*组织*需要控制和维护的信息（3.1）以及包含这些信息的媒介

条目注释1。记录的信息可以是任何格式和媒体，以及来自任何来源。条目注释2。记载的信息可以

指。

— *管理系统*（3.4），包括相关*过程*（3.9）。

— 为组织运作而创建的信息（文件）。

— 取得成果的证据（记录）。

3.12
业绩
可衡量的结果

条目注释1。业绩可以与定量或定性的调查结果有关。

条目注释2。绩效可以涉及到管理活动、*流程*（3.9）、产品、服务、系统或
组织（3.1）。

3.13
持续改进
提高*业绩*的经常性活动（3.12）。

3.14
效益
计划活动的实现程度和计划成果的实现程度

3.15
要求
陈述的、一般暗示的或强制性的需要或期望

条目注1。"一般暗示"是指该*组织*的习惯或通常做法(3.1)和
有关各方（3.2），所考虑的需要或期望是隐含的。

条目注释2。规定的要求是指在*文件资料*中说明的要求（3.11）。

3.16
符合性
满足一项*要求*（3.15）。

3.17
不符合规定
不*符合要求*（3.15）。

3.18
纠正措施
采取行动，消除*不符合要求*的原因（3.17），防止再次发生。

如需获取认证规则全文请与以下联系人联系：

蒋老师，联系电话：13826281695

或发函至邮箱获取：gdzj_101@163.com