INTERNATIONAL STANDARD

ISO 28000

Second edition
2022-03

Security and resilience — Security management systems — Requirements

Reference number
ISO 28000:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 11
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 plans 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 Improvement 18
10.1 Continual improvement 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.

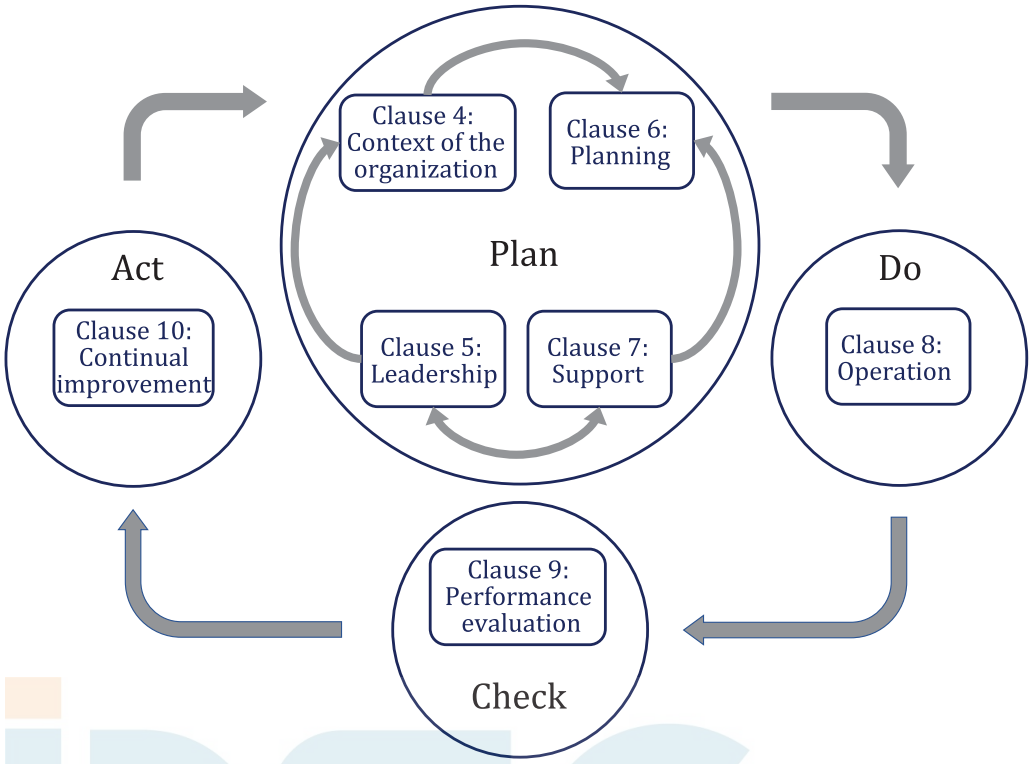

Figure 1 — PDCA model applied to the security management system

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* (3.7)

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

3.3
top management
person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.6) and *objectives* (3.7), as well as *processes* (3.9) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3.5
security management system
system of coordinated *policies* (3.6), *processes* (3.9) and practices through which an organization manages its security *objectives* (3.7)

3.6
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.3)

3.7
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product and *process* (3.9).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as a security objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *security management systems* (3.5), security objectives are set by the *organization* (3.1), consistent with the security *policy* (3.6), to achieve specific results.

3.8
risk
effect of uncertainty on *objectives* (3.7)

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

3.9
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

3.10
competence
ability to apply knowledge and skills to achieve intended results

3.11
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.4), including related *processes* (3.9);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.12
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.9), products, services, systems or *organizations* (3.1).

3.13
continual improvement
recurring activity to enhance *performance* (3.12)

3.14
effectiveness
extent to which planned activities are realized and planned results are achieved

3.15
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.11).

3.16
conformity
fulfilment of a *requirement* (3.15)

3.17
nonconformity
non-fulfilment of a *requirement* (3.15)

3.18
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.17) and to prevent recurrence

3.19
audit
systematic and independent *process* (3.9) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.20
measurement
process (3.9) to determine a value

3.21
monitoring
determining the status of a system, a *process* (3.9) or an activity

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its security management system including the requirements of its supply chain.

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

The organization shall determine:

— the interested parties that are relevant to the security management system;

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the security management system.

4.2.2 Legal, regulatory and other requirements

The organization shall:

a) implement and maintain a process to identify, have access to and assess the applicable legal, regulatory and other requirements related to its security;

b) ensure that these applicable legal, regulatory and other requirements are taken into account in implementing and maintaining its security management system;

c) document this information and keep it up to date;

d) communicate this information to relevant interested parties as appropriate.

ISO 28000-2022

国际标准

ISO/TS
28000

第2版
2022-03-15

安全与韧性 安全管理体系 要求

Security and resilience — Security management systems — Requirements

ISO 28000：2022

目次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 组织环境 4

4.1 理解组织及其环境 4

4.2 理解相关方的需求和期望 4

4.2.1 总则 4

4.2.2 法律法规和其他要求 4

4.2.3 原则 4

4.3 确定安全管理体系的范围 6

4.4 安全管理体系 6

5 领导作用 6

5.1 领导作用和承诺 6

5.2 安全方针 7

5.2.1 建立安全方针 7

5.2.2 安全方针要求 7

5.3 岗位、职责和权限 7

6 策划 7

6.1 应对风险和机遇的措施 7

6.1.1 总则 7

6.1.2 确定与安全有关的风险并确定机遇 8

6.1.3 应对与安全有关的风险和利用机遇 8

6.2 安全目标及其实现的策划 8

6.2.1 建立安全目标 8

6.2.2 确定安全目标 9

6.3 变更的策划 9

7 支持 .....

7.1 资源 9

7.2 能力 9

7.3 意识 …… 10
7.4 沟通 …… 10
7.5 成文信息 …… 10
7.5.1 总则 …… 10
7.5.2 创建和更新 …… 10
7.5.3 成文信息的控制 …… 11
8 运行 …… 11
8.1 运行的策划和控制 …… 11
8.2 确定过程和活动 …… 11
8.3 风险评估和应对 …… 11
8.4 控制 …… 12
8.5 安全策略、程序、过程和应对方法 …… 12
8.5.1 确定和选择战略和应对方法 …… 12
8.5.2 资源要求 …… 12
8.5.3 应对的实施 …… 13
8.6 安全计划 …… 13
8.6.1 总则 …… 13
8.6.2 响应结构 …… 13
8.6.3 警告和沟通 …… 13
8.6.4 安全计划的内容 …… 14
8.6.5 恢复 …… 14
9 绩效评价 …… 14
9.1 监视、测量、分析和评价 …… 14
9.2 内部审核 …… 15
9.2.1 总则 …… 15
9.2.2 内部审核方案 …… 15
9.3 管理评审 …… 15
9.3.1 总则 …… 15
9.3.2 管理评审输入 …… 15
9.3.3 管理评审输出 …… 16
10 改进 …… 16
10.1 持续改进 …… 16
10.2 不符合和纠正措施 …… 16
参考文献 …… 1

前言

国际标准化组织（ISO）是由各国标准化团体（ISO成员团体）组成的世界性的联合会。制定国际标准工作通常由ISO的技术委员会完成。各成员团体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与ISO保持联系的各国际组织（官方的或非官方的）也可参加有关工作。ISO与国际电工委员会（IEC）在电工技术标准化方面保持密切合作的关系。

制定本标准及其后续标准维护的程序在ISO/IEC指引 第1部分均有描述。应特别注意用于各不同类别ISO文件批准准则。本标准根据ISO/IEC导则第2部分的规则起草（见www.iso.org/directives）。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意。ISO不负责识别任何这样的专利权问题。在标准制定期间识别的专利权细节将出现在引言/或收到的ISO专利权声明清单中（www.iso.org/patents）。

ISO与合格评定相关的特定术语和表述含义的解释以及ISO遵循的世界贸易组织（WTO）贸易技术壁垒（TBT）原则相关信息访问以下URLL：www.iso.org/iso/foreword.html.

本标准由ISO/TC 292安全与韧性分委员会制定。

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章中加入了关于原则的建议，以便与ISO31000更好地协调；

——在第8章中增加了建议，以便与ISO22301更好地保持一致，促进整合，包括：

- 安全策略、程序、过程和应对；
- 安全计划。

有关本标准的任何反馈应直接向用户所在国家标准机构提出，这些机构的完整名单可以www.iso.org/members.html中找到。

引言

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，他们希望在其管理体系内系统地解决这些问题。正式的安全管理方法可以直接增进组织的业务能力和可信度。

本标准规定了安全管理体系要求，包括对供应链安全保证至关重要的方面。它要求组织：

——评估其运营的安全环境，包括其供应链(包括依赖关系和相互依存关系)；

——确定是否有足够的安全措施来有效管理与安全相关的风险；

——管理组织对法律法规和自愿义务的遵守情况；

——协调安全过程和控制，包括供应链的相关上游和下游过程和控制，以满足组织的目标。

安全管理与业务管理的许多方面相关联。它们包括组织控制或影响的所有活动(包括但不限于对供应链产生影响的活动)。应考虑对组织安全管理有影响的所有活动、职能和业务，包括(但不限于)其供应链。

关于供应链，必须考虑到供应链本质上是动态的。因此，一些管理多个供应链的组织可能希望其供方满足相关的安全标准，作为纳入该供应链的条件，以满足安全管理的要求。

本标准将策划-实施-检查-处置(PDCA)模式应用于组织策划、建立、实施、运行、监视、评审、保持和持续改进安全管理体系的有效性，见表1和图1。

表1：PDCA模型的解释

策划(建立)	建立与改进安全相关的安全方针、目标、指标、控制措施、过程和程序，以提供符合组织总方针和目标的结果。
实施(执行和运行)	执行和运行安全方针、控制措施、过程和程序。
检查(监视和评审)	根据安全方针和目标监视和评审绩效，向管理层报告结果以供评审，并确定和授权补救和改进措施。
处置(保持和改进)	根据管理评审的结果，通过采取纠正措施，保持和改进安全管理体系，并重新评价安全管理体系的范围和安全方针和目标。

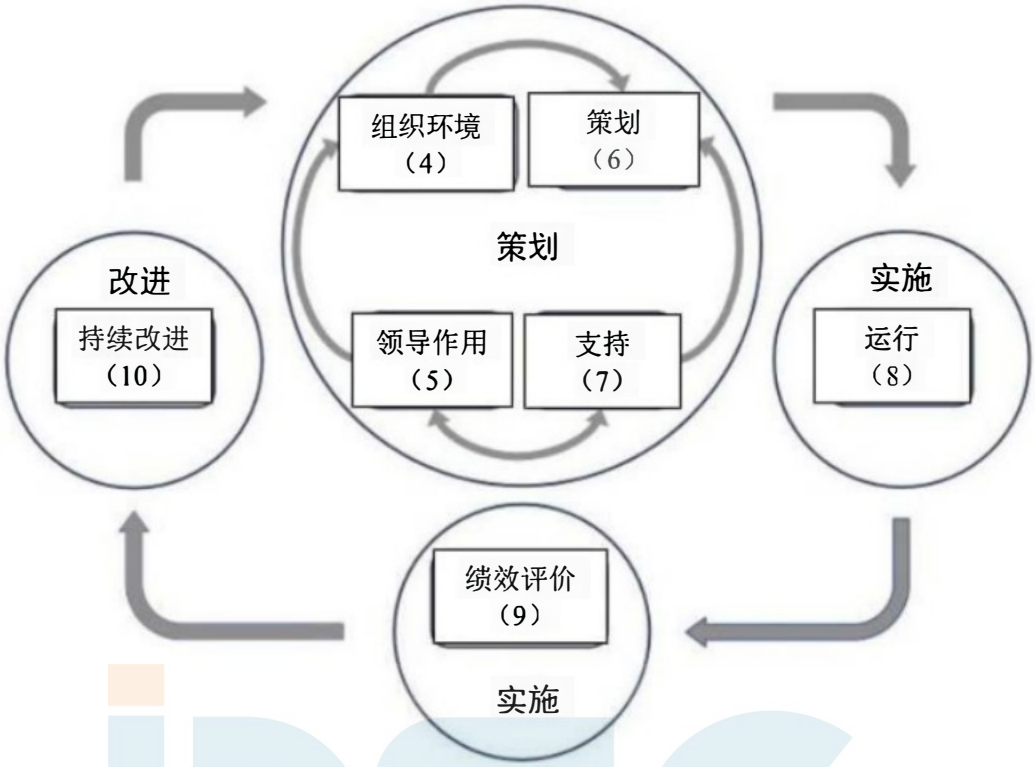

图1：应用于安全管理体系的PDCA模式

这确保了与其他管理体系标准的一致性，如ISO 9001、ISO 14001、ISO 22301、ISO/IEC 27001、ISO 45001等，从而支持与相关管理体系的一致和整合实施和运行。

对于有此愿望的组织，可以通过外部或内部审核程序来验证安全管理体系与本标准的一致性。

安全与韧性—安全管理体系—要求

1 范围

本标准规定了安全管理体系要求，包括与供应链相关的方面。

本标准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），旨在建立、实施、保持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。

本标准可以在组织整个生命周期中使用，并可应用于任何层级的内部或外部活动。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

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标准。

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：https://www.iso.org/obr

IEC 在线电工术语库：http://www.electropedia.org/

3.1

组织 organization

为实现目标，由职责、权限和相互关系构成自身功能的一个人或一组人。

注：组织包括但不限于企事业单位、政府机构、社团、个体工商户，或者上述组织的某部分或其组合，无论其是否为法人组织、公有或私有。

3.2

相关方（利益相关方） interested party; stakeholder

可影响或者受到决策或活动所影响，或者自认为受决策或活动影响的个人或组织。

示例：相关方可包括顾客、游客、居民、社区、供方、监管部门、非政府组织、投资方和工作人员。

3.3

最高管理者 top management

在最高层指挥和控制组织的一个人或一组人。

如需要获取全文

请联系北京三星九千认证中心有限公司技术部

联系电话:010-64429578-612

邮箱:duqq@sanxing9000.com