INTERNATIONAL STANDARD

ISO 28000

Second edition
2022-03

Security and resilience — Security management systems — Requirements

安全与韧性 — 安全管理体系 — 要求

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

目录

前言

国际标准化组织（ISO，the International Organization for Standardization）是由各国标准机构（ISO 成员机构）组成的全球性联合会。国际标准的制定工作通常由 ISO 技术委员会开展。对某一技术委员会所负责主题感兴趣的各成员机构，有权派代表参与该委员会的工作。与 ISO 相关的国际组织、政府机构和非政府机构，也可参与此项工作。在电工标准化的所有事务方面，ISO 与国际电工委员会（IEC，the International Electrotechnical Commission）密切合作。

本文件制定及后续维护所采用的程序，在《ISO/IEC 指令 第 1 部分》中有详细说明。其中需特别注意，不同类型文件所需的不同批准标准。本文件是依据《ISO/IEC 指令 第 2 部分》的编辑规则获得批准的（详情见 www.iso.org/directives ）。

需注意的是，本文件的某些内容可能涉及专利权问题。ISO 不负责识别任何或所有此类专利权。本文件制定过程中确定的任何专利权详情，将在引言和/ISO 收到的专利声明清单中说明（详情见 www.iso.org/patents ）。

本文件中出现的任何商号，仅为方便用户提供信息，不构成认可。

如需了解标准的自愿性本质、ISO 特定术语及与合格评定相关表述的含义，以及 ISO 遵守世界贸易组织（WTO，the World Trade Organization）《技术性贸易壁垒（TBT，Technical Barriers to Trade）》原则的相关信息，可查阅 www.iso.org/iso/foreword.html 。

本文件由 ISO/TC 292 技术委员会（安全与韧性，Security and resilience）编制。

本第二版取代并废止第一版（ISO 28000:2007 ），第二版经过了技术修订，但保留了现有要求，以便为使用先前版本的组织提供连续性。主要变化如下：

在第 4 条中增加了有关原则的建议，以更好地与 ISO 31000 协调一致；
在第 8 条中增加了相关建议，以更好地与 ISO 22301 保持一致，促进整合，包括：
安全策略、程序、流程及处理措施；
安全计划。

如有关于本文件的任何反馈或疑问，应提交给用户所在国家的标准机构。这些机构的完整列表可在 www.iso.org/members.html 查阅。

引言

大多数组织都面临着安全环境中日益增长的不确定性和波动性。因此，它们面临着影响其目标实现的安全问题，而这些问题需要在其管理体系内得到系统性解决。正规的安全管理方法能够直接提升组织的业务能力和可信度。

本文件规定了安全管理体系的要求，包括对供应链安全保障至关重要的那些方面。它要求组织：

评估其运营所处的安全环境，包括其供应链（涵盖依赖关系和相互依赖关系）；
确定是否已采取充分的安全措施，以有效管理与安全相关的风险；
管理组织所遵循的法定、监管及自愿性义务的合规情况；
使安全流程和控制（包括供应链的相关上游及下游流程和控制）与组织目标保持一致。

安全管理与业务管理的诸多方面相互关联。它涵盖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。所有活动、职能和运营都应被视为会对组织（包括但不限于其供应链）的安全管理产生影响。

关于供应链，必须认识到供应链本质上是动态变化的。因此，一些管理多条供应链的组织可能会要求其供应商满足相关安全标准，将此作为纳入该供应链的条件，以满足安全管理要求。

本文件运用计划 - 执行 - 检查 - 改进（PDCA，Plan - Do - Check - Act ）模型，对组织安全管理体系的规划、建立、实施、运行、监测、评审、维护以及持续改进其有效性进行规范，详见表 1 和图 1（因原文未给出图 1 内容，此处按原文翻译 ）。

表 1 — PDCA 模型说明

阶段	具体内容
计划（建立）	制定与改进安全相关的安全策略、目标、指标、控制措施、流程和程序，以实现与组织整体政策和目标相一致的结果。
执行（实施和运行）	实施并运行安全策略、控制措施、流程和程序。
检查（监测和评审）	对照安全策略和目标监测并评审绩效，向管理层报告结果以供评审，确定并授权采取补救和改进措施。
改进（保持和改进）	根据管理评审结果采取纠正措施，重新评估安全管理体系的范围以及安全策略和目标，从而保持并改进安全管理体系。

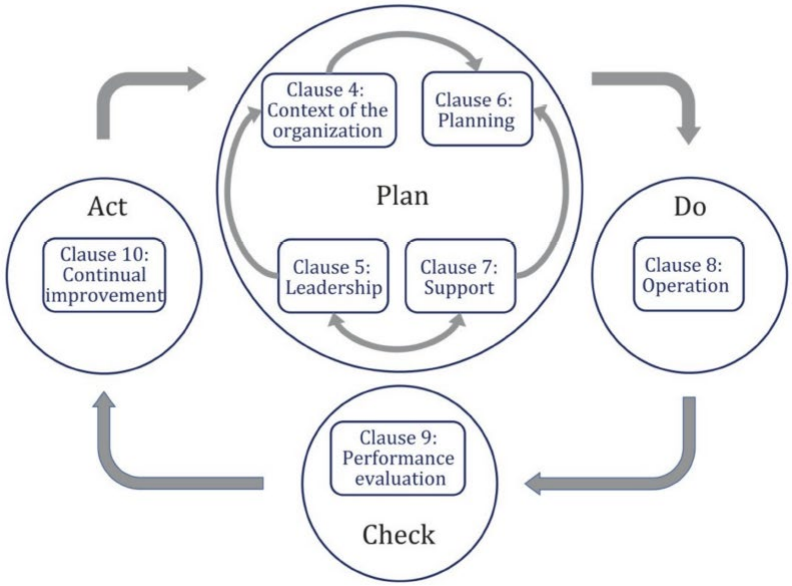

图 1 — 应用于安全管理体系的 PDCA 模型

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 ）在一定程度上保持一致性，从而支持与相关管理体系进行一致且整合的实施和运行。

对于有此需求的组织，安全管理体系与本文件的符合性可通过外部或内部审核过程进行验证。

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，涵盖与供应链相关的方面。

本文件适用于各类规模、各种类型的组织（如商业企业、政府或其他公共机构、非营利组织），这些组织有意建立、实施、保持并改进安全管理体系。它提供了一种全面通用的方法，不针对特定行业或领域。

本文件可在组织的整个生命周期内使用，且适用于所有层级的内部或外部活动。

2 规范性引用文件

以下文件在本文中被引用，其部分或全部内容构成本文件的要求。对于有日期的引用文件，仅引用的版本适用；对于无日期的引用文件，其最新版本（包括任何修订）适用。

ISO 22300《安全与韧性 — 词汇》

3 术语和定义

就本文件而言，采用 ISO 22300 中的术语和定义，以及以下术语和定义。

ISO 和 IEC 维护着用于标准化工作的术语数据库，可通过以下地址获取：

— ISO 在线浏览平台：https://www.iso.org/obp

— IEC 电子百科：https://www.electropedia.org/

3.1 组织（organization）

具有自身职能，通过职责、权限和关系来实现目标（3.7）的个人或人群。

注 1：组织的概念包括但不限于个体经营者、公司、企业、商行、事业单位、权威机构、合伙企业、慈善机构或机构，或其部分或组合，无论是否为法人实体，无论公立或私立。

注 2：若组织是更大实体的一部分，“组织”一词仅指该更大实体中处于安全管理体系（3.5）范围内的部分。

3.2 相关方（interested party，首选术语 ）；利益相关方（stakeholder，通用术语 ）

能够影响决策或活动、受决策或活动影响，或自认为受决策或活动影响的个人或组织（3.1） 。（因原文后续内容显示不全，翻译截至可见部分 ）

3.3 最高管理者（top management）

在最高层级指挥和控制组织（3.1）的个人或人群。

注 1：最高管理者有权在组织内委派职权并提供资源。

注 2：若管理体系（3.4）的范围仅涵盖组织的一部分，那么“最高管理者”指挥和控制该部分组织的人

员。

3.4 管理体系（management system）

组织（3.1）中相互关联或相互作用的一组要素，用于建立方针（3.6）和目标（3.7），以及实现这些目标的过程（3.9） 。

注 1：一个管理体系可针对单一领域或多个领域。

注 2：管理体系要素包括组织的结构、职责和权限、策划与运行。

3.5 安全管理体系（security management system）

组织用于管理其安全目标（3.7）的、由协调一致的方针（3.6）、过程（3.9）和实践构成的体系 。

3.6 方针（policy）

组织（3.1）最高管理者（3.3）正式表达的意图和方向 。

3.7 目标（objective）

要实现的结果。

注 1：目标可以是战略层面、战术层面或运营层面的。

注 2：目标可涉及不同领域（如财务、健康安全、环境 ），例如可以是组织整体层面的，也可以是特定项目、产品和过程（3.9）层面的。

注 3：目标可以通过其他方式表述，如预期结果、目的、运营准则、安全目标，或使用含义相近的词汇（如宗旨、目的、指标 ）。

注 4：在安全管理体系（3.5）语境下，安全目标由组织（3.1）制定，与安全方针（3.6）一致，以达成特定结果。

3.8 风险（risk）

不确定性对目标（3.7）的影响 。

注 1：影响是与预期的偏差，可能是正面、负面或两者兼具，可能带来、造成机会和威胁。

注 2：目标可涉及不同方面和类别，可应用于不同层级。

注 3：风险通常从风险来源、潜在事件、其后果及发生可能性方面进行表述。

3.9 过程（process）

一组相互关联或相互作用的活动，利用或转化输入以产生结果 。

注 1：过程的结果称为输出、产品还是服务，取决于引用的语境。

3.10 能力（competence）

运用知识和技能达成预期结果的能力

3.11 成文信息（documented information）

组织（3.1）需要控制和保持的信息，以及承载这些信息的媒介

注 1：成文信息可以是任何格式和媒介，来自任何来源。

注 2：成文信息可指：

— 管理体系（3.4），包括相关过程（3.9）；

— 组织为运营而创建的信息（文件）；

— 已实现结果的证据（记录）。

3.12 绩效（performance）

可测量的结果

注 1：绩效可以涉及定量或定性的结果。

注 2：绩效可以涉及管理活动、过程（3.9）、产品、服务、体系或组织（3.1）。

3.13 持续改进（continual improvement）

增强绩效（3.12）的重复性活动

3.14 有效性（effectiveness）

已策划活动得以实施、已策划结果得以实现的程度

3.15 要求（requirement）

明示的、通常隐含的或必须履行的需求或期望

注 1：“通常隐含”指对于组织（3.1）和相关方（3.2）而言，考虑的需求或期望是不言而喻的惯例或常规做法。

注 2：特定要求是指明示的要求，例如在成文信息（3.11）中规定的要求。

3.16 合规（conformity）

满足要求（3.15）

3.17 不合规（nonconformity）

未满足要求（3.15）

3.18 纠正措施（corrective action）

消除不合规（3.17）的原因以防止再发生的行动

3.19 审核（audit）

为获得证据并对其进行客观评价，以确定满足审核准则的程度所进行的系统的、独立的过程（3.9）

注 1：审核可以是内部审核（第一方）或外部审核（第二方或第三方），也可以是结合审核（结合两个或多个领域）。

注 2：内部审核由组织（3.1）自身进行，或由外部方代表组织进行。

注 3：“审核证据”和“审核准则”在 ISO 19011 中定义。

3.20 测量（measurement）

确定数值的过程（3.9）

3.21 监视（monitoring）

确定体系、过程（3.9）或活动的状态

注 1：为确定状态，可能需要检查、监督或批判性观察。

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关并影响其实现安全管理体系预期结果能力的内外部问题，包括其供应链的要求。

组织应确定气候变化是否是一个相关事项。

4.2 理解相关方的需求和期望

4.2.1 总则

组织应确定：

— 与安全管理体系相关的相关方；

— 这些相关方的相关要求；

— 哪些要求将通过安全管理体系予以解决。

4.2.2 法律、法规和其他要求

组织应：

a） 实施并保持一个过程，以识别、获取和评估适用的与安全相关的法律、法规和其他要求；

b） 确保在实施和保持安全管理体系时考虑这些适用的法律、法规和其他要求；

c） 记录这些信息并保持最新；

d） 适时将这些信息传达给相关方。

4.2.3 原则

4.2.3.1 总则

组织内安全管理的目的是创造价值，尤其是保护价值。

组织应用图 2 给出的、4.2.3.2 至 4.2.3.9 描述的原则。

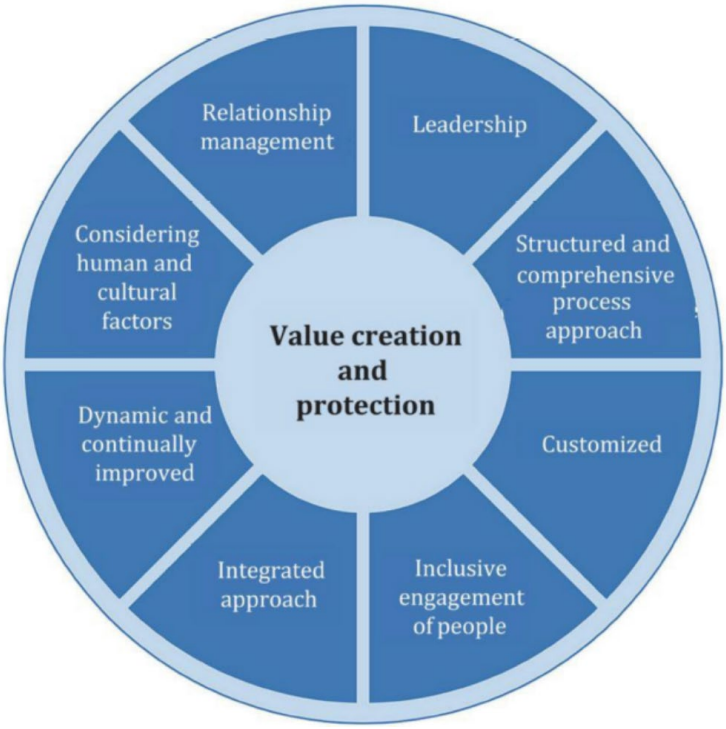

图 2 — 原则

核心：Value creation and protection（价值创造与保护 ）

外围原则：Relationship management（关系管理 ）、Leadership（领导力 ）、Structured and comprehensive process approach（结构化且全面的过程方法 ）、Customized（定制化 ）、Inclusive engagement of people（人员的广泛参与 ）、Integrated approach（综合方法 ）、Dynamic and continually improved（动态且持续改进 ）、Considering human and cultural factors（考量人文与文化因素 ） ，这些原则围绕价值创造与保护，构建安全管理体系相关理念 。

4.2.3.2 领导作用（Leadership）

各级领导者应确立统一的宗旨和方向。他们应创造条件，使组织的战略、方针、过程和资源与实现其目标保持一致。第 5 条解释了与该原则相关的要求。

4.2.3.3 基于现有最佳信息的结构化、全面过程方法（Structured and comprehensive process approach based on best available information）

对包括供应链在内的安全管理采用结构化、全面的方法，应有助于实现一致且可比的结果。当活动作为相互关联的过程、作为一个协调的系统来理解和管理时，能够更有效率和效果地达成这些结果。

4.2.3.4 定制化（Customized）

安全管理体系应根据组织的内外部环境和需求进行定制并与之相匹配，应与其目标相关联。

4.2.3.5 人员的广泛参与

组织应适时、恰当地让相关方参与。应充分考量他们的知识、观点和看法，以提升安全管理意识并为其提供助力。组织应确保各层级人员都能得到尊重并参与其中。

4.2.3.6 综合方法

安全管理是所有组织活动的有机组成部分，应与组织的其他所有管理体系相整合。

无论正式、非正式还是直观的组织风险管理，都应融入安全管理体系。

4.2.3.7 动态且持续改进

组织应持续关注通过学习和实践来改进，以维持绩效水平，应对内外部环境变化，并创造新机遇。

4.2.3.8 考量人文与文化因素

人类行为和文化对安全管理各方面影响重大，应在各个层面和环节加以考量。决策应基于数据和信息的分析与评估，以确保决策更具客观性、信心，更可能产生预期结果，同时也应考虑个体看法。

4.2.3.9 关系管理

为实现持续成功，组织应管理与所有相关方的关系，因其可能影响组织绩效。

注：相关方可能提出与气候变化相关的要求。

4.3 确定安全管理体系的范围

组织应明确安全管理体系的边界和适用性，以确立其范围。

确定范围时，组织应考量：

— 4.1 提及的内外部问题；

— 4.2 提及的要求。

范围应形成成文信息。

若组织将影响安全管理体系合规性的过程外包，应确保这些过程受控制。外包过程所需的控制措施及职责，应在安全管理体系中明确。

4.4 安全管理体系

组织应依据本文件要求，建立、实施、保持并持续改进安全管理体系，涵盖所需过程及其相互作用。

5 领导力

5.1 领导力与承诺

最高管理者应通过以下方式，展现对安全管理体系的领导力和承诺：

— 确保建立安全方针和目标，且与组织战略方向相符；

— 确保识别并监测组织相关方的要求和期望，及时采取行动管理这些期望，将安全管理体系要求融入组织业务流程；

— 确保安全管理体系要求融入组织业务流程；

— 确保安全管理体系所需资源可用；

— 传达有效安全管理及符合安全管理体系要求的重要性；

— 确保安全管理体系达成预期结果；

— 确保安全管理目标、指标和方案切实可行；

— 确保组织其他部门产生的安全方案与安全管理体系互补；

— 指导和支持人员为安全管理体系有效性做贡献；

— 推动组织安全管理体系持续改进；

— 支持其他相关角色在其职责范围内展现领导力。

注：本文件中“业务”可广义理解为组织存在目的的核心活动。

5.2 安全方针

5.2.1 建立安全方针

最高管理者应建立安全方针，需：

a） 契合组织宗旨；

b） 为设定安全目标提供框架；

c） 承诺满足适用要求；

d） 承诺持续改进安全管理体系；

e） 考量安全方针、目标、指标、方案等对组织其他方面的不利影响。

5.2.2 安全方针要求

安全方针应：

— 与组织其他方针一致；

— 与组织整体安全风险评估一致；

— 在收购、合并或业务范围变化（可能影响安全管理体系连续性或相关性）时，可开展评审；

— 描述并分配对结果的主要责任和职责；

— 形成成文信息；

— 在组织内传达；

— 适时向相关方提供。

注：组织可制定详细的内部安全管理方针（含推动体系所需信息，部分可保密），以及摘要版（非保密）向相关方传播，涵盖广泛目标。

5.3 职责、权限和授权

最高管理者应确保相关角色的职责和权限在组织内得到分配并传达。

最高管理者应分配以下职责和权限：

a） 确保安全管理体系符合本文件要求；

b） 向最高管理者报告安全管理体系绩效。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

策划安全管理体系时，组织应考量 4.1 的问题和 4.2 的要求，确定需应对的风险和机遇，以：

— 确保安全管理体系达成预期结果；

— 预防或降低不良影响；

— 实现持续改进。

组织应策划：

a） 应对这些风险和机遇的措施；

b） 如何：

— 将措施整合并实施到安全管理体系过程中；

— 评估这些措施的有效性。

管理风险的目的是创造和保护价值，应融入安全管理体系。与组织及相关方安全相关的风险，在 8.3 中处理。

6.1.2 确定安全相关风险并识别机遇

确定安全相关风险、识别和利用机遇，需主动开展风险评估，应涵盖（但不限于 ）：

a） 物理或功能故障、恶意或犯罪行为；

b） 环境、人文和文化因素及其他内外部环境（含组织控制外影响安全的因素）；

c） 安全设备的设计、安装、维护和更换；

d） 组织的信息、数据、知识和沟通管理；

e） 与安全威胁和漏洞相关的信息；

f） 供应商间的相互依赖关系。

6.1.3 应对安全相关风险并利用机遇

对已识别安全相关风险的评估，应作为（但不限于）以下方面的输入：

a） 组织整体风险管理；

b） 风险处置；

c） 安全管理目标；

d） 安全管理过程；

e） 安全管理体系的设计、规范和实施；

f） 识别充足资源（含人员配置）；

g） 识别培训需求和所需能力水平。

6.2 安全目标及实现策划

6.2.1 建立安全目标

组织应在相关职能和层级建立安全目标。

安全目标应：

a） 与安全方针一致；

b） 可测量（可行时 ）；

c） 考量适用要求；

d） 可监测；

e） 可传达；

f） 适时更新；

g） 形成成文信息。

6.2.2 确定安全目标

策划实现安全目标时，组织应确定：

— 需开展的工作；

— 所需资源；

— 责任人员；

— 完成时间；

— 结果评估方式。

建立和评审安全目标时，组织应考量：

a） 技术、人力、行政及其他可选方案；

b） 相关方的观点及影响。

安全目标应与组织持续改进的承诺一致。

6.3 变更策划

组织确定需变更安全管理体系（含条款 10 识别的变更）时，应按策划实施变更。

组织应考量：

a） 变更目的及潜在后果；

b） 安全管理体系的完整性；

c） 资源可用性；

d） 职责和权限的分配或重新分配。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进安全管理体系所需资源。

7.2 能力

组织应：

— 确定在其控制下、影响安全绩效的人员所需的能力；

— 确保这些人员通过适当教育、培训或经验具备能力，且通过适当安全审查；

— 适用时，采取行动获取所需能力，并评估行动有效性。

应保留适当成文信息作为能力证据。

注：适用行动可包括，如提供培训、指导或重新分配现有人员；或招聘 / 签约有能力人员。

7.3 意识

在组织控制下工作的人员应知晓：

— 安全方针；

— 其对安全管理体系有效性的贡献，包括安全绩效提升的益处；

— 不遵守安全管理体系要求的后果；

— 其在达成安全管理方针、程序合规及满足安全管理体系要求（含应急准备与响应要求 ）中的角色和

职责。

7.4 沟通

组织应确定与安全管理体系相关的内外部沟通内容，包括：

— 沟通的信息；

— 沟通时机；

— 沟通对象；

— 沟通方式；

— 信息传播前的敏感性考量。

7.5 成文信息

7.5.1 总则

组织的安全管理体系应包含：

a） 本文件要求的成文信息；

b） 组织确定的、对安全管理体系有效性必要的成文信息。

成文信息应描述实现安全管理目标和指标的职责与权限，包括达成这些目标和指标的方法与时间安排。

注：安全管理体系成文信息的详略程度因组织而异，取决于：

— 组织规模、活动、过程、产品和服务类型；

— 过程及其相互作用的复杂性；

— 人员能力。

组织应确定信息价值，建立所需完整性级别及防止未经授权访问的安全控制。

7.5.2 成文信息的创建和更新

创建和更新成文信息时，组织应确保适当：

— 标识和描述（如标题、日期、作者、参考编号）；

— 格式（如语言、软件版本、图形 ）和媒介（如纸张、电子）；

— 适用性和充分性的评审与批准。

7.5.3 成文信息的控制

安全管理体系和本文件要求的成文信息应受控，以确保：

a） 在需要时、需要处可用且适用；

b） 充分保护（如防止泄密、不当使用或完整性丢失）；

c） 必要时定期评审、修订，并由授权人员批准其充分性；

d） 作废文件、数据和信息从所有发放点和使用点及时移除，或确保不被误使用；

e） 因法律或知识保存目的留存的归档文件、数据和信息，已适当标识。

对于成文信息的控制，组织应按需开展以下活动：

— 分发、访问、检索和使用；

— 存储和保存，包括可读性保护；

— 变更控制（如版本控制）；

— 留存和处置。

组织确定的、对安全管理体系策划和运行必要的外部来源成文信息，应适当识别并受控。

注：访问可指仅允许查看成文信息的权限决定，或允许查看和修改成文信息的权限与授权决定。

8 运行

8.1 运行策划和控制

组织应策划、实施和控制满足要求及实施条款 6 确定措施所需的过程，方式为：

— 建立过程准则；

— 依据准则实施过程控制。

成文信息应按需提供，以确保过程按策划执行。

8.2 过程和活动的识别

组织应识别达成以下目标所需的过程和活动：

a） 符合其安全方针；

b） 符合法律、法规和监管安全要求；

c） 其安全管理目标；

d） 交付其安全管理体系；

e） 供应链所需的安全级别。

8.3 风险评估和处置

组织应实施并保持风险评估和处置过程。

注：风险评估和处置过程在 ISO 31000 中规定。

组织应：

a） 识别安全相关风险，按安全管理所需资源确定优先级；

b） 分析和评价已识别风险；

c） 确定哪些风险需要处置；

d） 选择并实施应对这些风险的方案；

e） 编制并实施风险处置计划。

注：本款风险与组织及相关方安全相关，管理体系有效性相关风险和机遇在 6.1 中处理。

8.4 控制措施

8.2 所列设计应包含人力资源管理控制，以及安全相关设备、仪器和信息技术项目的设计、安装、运行、翻新和修改（适用时）。若修订现有安排或引入新安排可能影响安全管理，组织应在实施前考虑相关安全风险。需考虑的新安排或修订安排包括：

a） 修订的组织结构、角色或职责；

b） 培训、意识和人力资源管理；

c） 修订的安全管理方针、目标、指标或方案；

d） 修订的过程和程序；

e） 引入新的基础设施、安全设备或技术（可能含硬件和 / 或软件 ）；

f） 适用时引入新承包商、供应商或人员；

g） 外部供应商的安全保障要求。

组织应控制策划的变更，评审意外变更的后果，必要时采取行动减轻不利影响。

组织应确保与安全管理体系相关的外部提供过程、产品或服务受控。

8.5 安全策略、程序、过程和处置

8.5.1 策略和处置的识别与选择

组织应实施并保持系统过程，分析与安全相关的漏洞和威胁。基于漏洞与威胁分析及后续风险评估，组织应识别并选择包含一个或多个程序、过程和处置的安全策略。

识别应基于策略、程序、过程和处置在以下方面的程度：

a） 维持组织安全；

b） 降低安全漏洞发生可能性；

c） 降低威胁实际发生可能性；

d） 缩短安全处置缺陷的周期并限制其影响；

e） 确保充足资源可用。

选择应基于策略、过程和处置在以下方面的程度：

— 满足保护组织安全的要求；

— 考量组织可能承担或不承担的风险数量和类型；

— 考量相关成本和收益。

8.5.2 资源要求

组织应确定实施所选安全程序、过程和处置的资源需求。

8.5.3 处置的实施

组织应实施并保持所选安全处置。

8.6 安全计划

8.6.1 总则

组织应基于所选策略和处置，建立并形成文件化的安全计划和程序。组织应实施并保持响应架构，确保向相关方及时有效通报与安全相关的漏洞、紧迫安全威胁或持续安全违规情况。响应架构应提供计划和程序，以在面临紧迫安全威胁或持续安全违规时管理组织。

8.6.2 响应架构

组织应实施并保持架构，明确指定人员或一个/多个团队，负责应对与安全相关的漏洞和威胁。指定人员或每个团队的角色与职责，以及人员或团队间的关系，应清晰识别、传达并形成文件。

这些团队总体应具备以下能力：

a） 评估安全威胁的性质、范围及其潜在影响；

b） 评估影响是否达到触发正式响应的预定义阈值；

c） 启动适当安全响应；

d） 策划需开展的行动；

e） 以生命安全为首要优先级确定行动优先级；

f） 监测与安全相关漏洞的变化影响、威胁行为者意图和能力的变化、安全违规及组织响应；

g） 启动安全处置；

h） 与相关方、主管部门和媒体沟通；

i） 为沟通管理贡献沟通计划。

对于每个指定人员或团队，应：

— 识别具备必要职责、权限和能力的人员（含替补 ），以履行指定角色；

— 形成文件化程序，指导其行动（含响应的启动、运行、协调和沟通 ）。

8.6.3 预警和沟通

组织应形成文件化并保持程序，用于：

a） 向内部和外部相关方沟通（含沟通内容、时机、对象和方式 ）；

注：组织可形成文件化程序，规定与员工及其紧急联系人沟通的方式和情形。

b） 接收、形成文件化并响应来自相关方的沟通（含任何国家或地区风险咨询系统或等效系统）；

c） 确保安全违规、漏洞或威胁期间沟通手段可用；

d） 促进与安全威胁和/或违规响应者的结构化沟通；

e） 提供安全违规后组织媒体响应的细节（含沟通策略）；

f） 记录安全违规细节、采取的行动和做出的决策。

适用时，还应考虑并实施：

— 向可能受实际或紧迫安全违规影响的相关方发出警报；

— 确保多个响应组织间适当协调与沟通。

预警和沟通程序应作为组织测试和培训计划的一部分进行演练。

8.6.4 安全计划的内容

组织应形成文件化并保持安全计划。这些计划应提供指导和信息，协助团队应对安全漏洞、威胁和/或违规，协助组织响应并恢复安全。

安全计划总体应包含：

a） 团队为实现以下目标将采取行动的细节：

1） 维持或恢复商定的安全状态；

2） 监测实际或紧迫安全威胁、漏洞或违规的影响及组织响应；

b） 预定义阈值的参考及启动响应的流程；

c） 恢复组织安全的程序；

d） 管理安全漏洞、威胁或实际/紧迫安全违规直接后果的细节，应适当考量：

1） 人员福利；

2） 可能受损的资产、信息和人员价值；

3） 核心活动（进一步）损失或不可用的预防。

每个计划应包含：

— 目的、范围和目标；

— 实施计划的团队角色和职责；

— 实施解决方案的行动；

— 启动（含启动标准 ）、运行、协调和沟通团队行动所需信息；

— 内外部相互依赖关系；

— 资源需求；

— 报告要求；

— 解除响应的流程。

每个计划应在需要时、需要处可用且适用。

8.6.5 恢复

组织应形成文件化过程，以从安全违规期间及前后采取的任何临时措施中恢复组织安全。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

— 需监视和测量的内容；

— 适用时，监视、测量、分析和评价的方法（确保结果有效 ）；

— 监视和测量的实施时机；

— 监视和测量结果的分析与评价时机。

成文信息应作为结果证据提供。

组织应评价安全管理体系的绩效和有效性。

9.2 内部审核

9.2.1 总则

组织应按策划的间隔开展内部审核，以获取安全管理体系是否：

a） 符合：

1） 组织自身安全管理体系要求；

2） 本文件要求；

b） 有效实施和保持的信息。

9.2.2 内部审核方案

组织应策划、建立、实施和保持审核方案（含频率、方法、职责、策划要求和报告）。

建立内部审核方案时，组织应考虑相关过程的重要性及以往审核结果。

组织应：

a） 为每次审核定义审核目标、准则和范围；

b） 选择审核员并开展审核，确保审核过程的客观性和公正性；

c） 确保审核结果报告给相关管理者；

d） 验证安全设备和人员已适当部署；

e） 确保无不当延迟地采取必要纠正措施，消除检测到的不合规及原因；

f） 确保后续审核行动包括验证所采取行动及报告验证结果。

成文信息应作为审核方案实施和审核结果的证据提供。

审核方案（含任何日程）应基于组织活动的风险评估结果和以往审核结果。审核程序应涵盖范围、频率、方法和能力，以及开展审核和报告结果的职责与要求。

9.3 管理评审

9.3.1 总则

最高管理者应按策划的间隔评审组织的安全管理体系，确保其持续适宜性、充分性和有效性。

组织应考虑分析和评价结果及管理评审输出，确定是否存在与业务或安全管理体系相关的需求或机遇，作为持续改进的一部分加以解决。

注：组织可利用安全管理体系过程（如领导力、策划和绩效评价）实现改进。

9.3.2 管理评审输入

管理评审应包含：

a） 以往管理评审行动的状态；

b） 与安全管理体系相关的内外部问题变化；

c） 与安全管理体系相关的相关方需求和期望变化；

d） 安全绩效信息，含趋势：

1） 不合规及纠正措施；

2） 监视和测量结果；

3） 审核结果；

e） 持续改进机遇；

f） 符合法律要求和组织遵循的其他要求的审核与评价结果；

g） 外部相关方的沟通（含投诉）；

h） 组织的安全绩效；

i） 目标和指标的达成程度；

j） 纠正措施的状态；

k） 以往管理评审的后续行动；

l） 变化的情况（含法律、法规和其他要求的发展，见 4.2.2 安全相关内容）；

m） 改进建议。

9.3.3 管理评审输出

管理评审结果应包含与持续改进机遇及安全管理体系变更需求相关的决策。

成文信息应作为管理评审结果的证据提供。

10 改进

10.1 持续改进

组织应持续改进安全管理体系的适宜性、充分性和有效性。组织应主动寻求改进机遇，即使未因与安全相关的漏洞及紧迫安全威胁或持续安全违规向相关方发出提示。

10.2 不合规和纠正措施

当发生不合规时，组织应：

a） 对不合规做出响应，适用时：

1） 采取行动控制和纠正不合规；

2） 处理后果；

b） 评价是否需要采取行动消除不合规原因（防止再发生或在其他地方发生 ），方式为：

1） 评审不合规；

2） 确定不合规原因；

3） 确定是否存在类似不合规或可能发生；

c） 实施所需行动；

d） 评审所采取纠正措施的有效性；

e） 必要时，变更安全管理体系。

纠正措施应与遇到的不合规影响相适配。

成文信息应作为以下证据提供：

— 不合规的性质及后续采取的行动；

— 任何纠正措施的结果；

— 与安全相关的调查：

— 故障（含未遂事件和误报警 ）；

— 事件和紧急情况；

— 不合规；

— 采取行动减轻此类故障、事件或不合规产生的后果。

程序应要求，除非立即实施可避免生命或公共安全的紧迫暴露，否则所有拟采取的纠正措施应在实施前通过安全相关风险评估过程评审。

为消除实际和潜在不合规原因采取的任何纠正措施，应与问题的严重程度适配，并与可能遇到的安全管理相关风险相称。

参考文献

[1] ISO 9001，质量管理体系 — 要求
[2] ISO 14001，环境管理体系 — 要求及使用指南
[3] ISO 19011，管理体系审核指南
[4] ISO 22301，安全与韧性 — 业务连续性管理体系 — 要求
[5] ISO/IEC 27001，信息技术 — 安全技术 — 信息安全管理体系 — 要求
[6] ISO 28001，供应链安全管理体系 — 实施供应链安全、评估和计划的最佳实践 — 要求及指南
[7] ISO 28002，供应链安全管理体系 — 供应链韧性发展 — 要求及使用指南
[8] ISO 28003，供应链安全管理体系 — 提供供应链安全管理体系审核和认证的机构的要求
[9] ISO 28004-1，供应链安全管理体系 — ISO 28000 实施指南 — 第 1 部分：一般原则
[10] ISO 28004-3，供应链安全管理体系 — ISO 28000 实施指南 — 第 3 部分：中小企业（海运港口除外）采用 ISO 28000 的额外特定指南
[11] ISO 28004-4，供应链安全管理体系 — ISO 28000 实施指南 — 第 4 部分：若将符合 ISO 28001 作为管理目标时，实施 ISO 28000 的额外特定指南
[12] ISO 31000，风险管理 — 指南
[13] ISO 45001，职业健康安全管理体系 — 要求及使用指南
[14] ISO 指南 73，风险管理 — 词汇