ICS 03.100.01
CCS A 90

中华人民共和国国家标准

GB/T 40753—2021/ISO 28004:2007

供应链安全管理体系 ISO 28000 实施指南

Security management systems for the supply chain—Guidelines for the implementation of ISO 28000

(ISO 28004:2007,IDT)

2021-11-26 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件使用翻译法等同采用了 ISO 28004:2007《供应链安全管理体系规范 ISO 28000 实施指南》。本文件做了下列最小限度的编辑性修改：

——增加部分列项引导语；

——增加资料性附录 A。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国公共安全基础标准化技术委员会(SAC/TC 351)提出并归口。

本文件起草单位：中国标准化研究院、南京卫岗乳业有限公司、福建你他共创网络科技有限公司、国网山东省电力公司、中国质量认证中心、方圆标志认证集团有限公司、北京城市系统工程研究中心、中国网络安全审查技术与认证中心。

本文件主要起草人：秦挺鑫、白元龙、叶耀华、孙世军、潘英、宋跃炜、王晶晶、张剑、魏军、韩智海、陈伟、朱琳、谭玲。

引　言

ISO 28000:2007《供应链安全管理体系规范》和本文件根据建立公认的供应链管理体系标准这一需求制定，可用作安全管理体系评价和认证依据，也可指导此类标准的实施。

ISO 28000 与 GB/T 19001 和 GB/T 24001 管理体系标准兼容。这些标准促进了组织根据自身意愿对质量、环境和供应链管理体系进行整合。

本文件在各条款/分条款前有一个方框，列出了 ISO 28000 中的完整要求，随后是相关的指导。本文件条款号与 ISO 28000 的条款号相一致。

本文件将进行适当评审或修改。ISO 28000 修订时将进行评审。

本文件未包括针对供应链运营商、供应商和利益相关方之间合同的所有必要的规定。因此，使用者宜合理采用本文件。

遵守本文件本身并不意味着免除法律义务。

供应链安全管理体系　ISO 28000 实施指南

1　范围

本文件为 ISO 28000:2007《供应链安全管理体系规范》的应用提供通用性建议。

本文件解释了 ISO 28000 中的基本原则，对 ISO 28000 各项要求的目的、典型输入、过程和典型输出进行了说明，旨在帮助理解和实施 ISO 28000。

本文件在 ISO 28000 条款之外不再产生附加要求，也未规定实施 ISO 28000 的强制性方法。

ISO 28000

1　范围

本国际标准规定了安全管理体系(包括对供应链安全保证至关重要的方面)的要求。这些方面包括但不限于金融、制造、信息管理以及商品的包装、储存和在不同运输方式和地点之间的转运。安全管理与企业管理的许多其他方面存在联系。在任何影响安全管理的期间或地点，包括在采用供应链运输货物时，应直接考虑这些其他方面。

本文件适用于在生产或者供应链任何阶段希望达成以下目标的从制造、服务、存储或者运输的任何规模的组织(从小型到跨国规模)：

a)　建立、实施、维护和改进安全管理体系；

b)　确保符合规定的安全管理策略；

c)　验证是否符合其他要求；

d)　寻求通过授权的第三方认证组织对其安全管理体系进行认证或注册；

e)　对于本国际标准的合规性做出自我决定和声明。

一些法规以及监管规范也对在本文件中某些要求进行了阐述。

本文件并非旨在要求对合规性进行重复验证。

选择第三方认证的组织可进一步证明其在促进供应链安全方面的重要努力。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

ISO 28000 中的术语和定义及以下术语和定义适用于本文件。

ISO 28000

3 术语和定义

3.1

设施 facility

厂房、机械、物业、建筑、车辆、船舶、港口设施及其他具有具体可量化业务功能和服务的基础设施项目或者厂房和相关系统。

注：该定义规定了对于实现安全和应用安全管理至关重要的任何软件代码。

3.2

安全 security

针对旨在对供应链造成损坏或破坏或由供应链造成损坏或破坏的故意行为的抵抗力。

3.3

安全管理 security management

组织借以对风险、相关潜在威胁及其影响进行最佳管理的系统性和协调性活动。

3.4

安全管理目标 security management objective

为满足安全管理策略而要求实现的具体安全成果或成就。

注：对于在客户或者最终用户所有业务中产品、供货或服务，上述成果与这些存在直接或间接联系。

3.5

安全管理方针 security management policy

组织与安全以及安全相关流程和活动管理用框架相关的总体目的和方向；其中，上述流程和活动源于并符合该组织的政策和监管要求。

3.6

安全管理计划 security management programmes

实现安全管理目标的方式。

3.7

安全管理指标 security management target

为实现安全管理目标所需要达到的性能水平。

3.8

利益相关方 stakeholder

在组织效能、成功或活动影响方面拥有既得利益的个人或实体。

注：包括客户、股东、金融组织、保险组织、监管组织、法定组织、员工、承包商、供应商、劳工组织或者协会。

3.9

供应链 supply chain

从原材料来源到通过运输途径将产品或者服务交付至终端用户的一系列资源和流程。

注：供应链可包括供应商、生产设施、物流供应商、内部集散中心、经销商、批发商及其他通向最终用户的实体。

3.9.1

下游 downstream

在货物离开组织的直接运行控制后(包括但不限于保险、财务、数据管理以及货物的包装、储存和转运)供应链中货物的操作、流程和移动情况。

3.9.2

上游　upstream

在货物进入组织的直接运行控制前(包括但不限于保险、财务、数据管理以及货物的包装、储存和转运)供应链中货物的操作、流程和移动情况。

3.10

最高管理者　top management

指导和控制某组织的最高层次人员或人员团体。

注：尤其在大型跨国组织，最高管理者并非如本文件所述亲自参与；同时，应明确最高管理者在行政管理体系中的职责。

3.11

持续改进　continual improvement

为了按组织安全策略改进总体安全性能而增强安全管理体系的重复性流程。

3.1

风险　risk

产生安全威胁的可能性及其后果。

3.2

安全排查　security cleared

验证接触安全敏感材料人员可信度的过程。

3.3

威胁　threat

对利益相关方、设施、运行、供应链、社会、经济或业务连续性和完整性造成潜在危害的任何蓄意行为或一系列行为。

4　安全管理体系要素

成功安全管理的要素见图1。

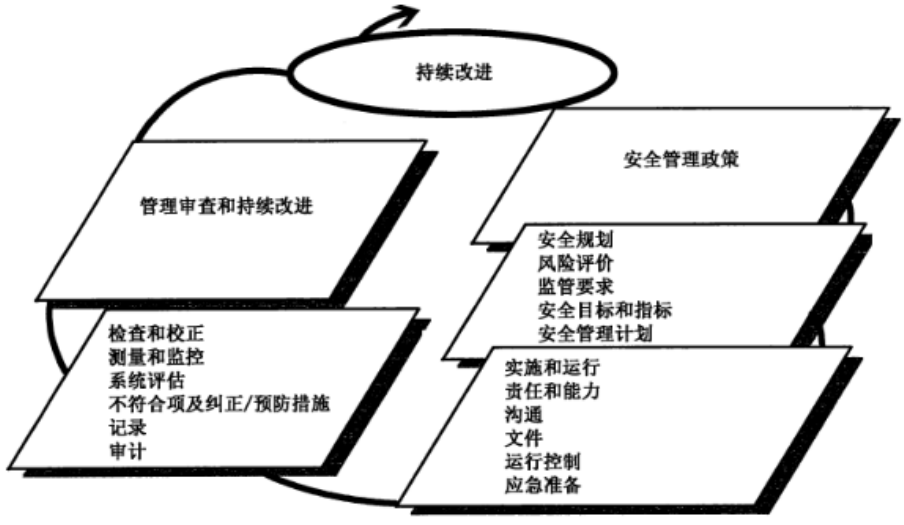

图1　成功安全管理的要素

4.1 通用要求

通用要求涉及以下方面。

a) ISO 28000 要求

组织应建立、制定、实施、维护和不断改进有效的安全管理体系，以确定安全威胁、评价风险、控制并减轻其后果。 组织应按照第 4 章的要求不断提高系统的有效性。 组织应确定其安全管理体系的范围。若组织选择将影响满足这些要求的任何流程外包，则该组织应保证这些流程处于管控下。在安全管理体系之内，应确定对这些外包流程的必要控制措施和责任。

b) 目的

组织宜建立并维持符合 ISO 28000 所有要求的管理体系。这有助于组织满足安全规范、要求和法律的规定。

安全管理体系详细程度和复杂度、文件范围和投入的资源取决于组织的规模和复杂度及其活动的性质。

组织有权自行灵活确定管理体系的边界和范围，可选择在整个组织内、组织具体的运行单位或活动中实施 ISO 28000。

在确定管理体系的边界和范围时宜予以注意。组织不得试图通过限定其范围来规避对组织整体运行所需的某项运行或活动，或可能对员工及其他利益相关方造成影响的那些运行或活动的评价。

当在具体的运行单位或活动中实施 ISO 28000 时，组织其他部分制定的安全策略和程序也可用于具体的运行单位或活动，以便满足 ISO 28000 的要求。这就要求对这些安全策略或程序进行略微修订或修正，以确保其适用于具体的运行单位或活动。

c) 典型输入

所有输入要求均在 ISO 28000 中作出了规定。

d) 典型输出

典型输出是一个得以有效实施和保持的安全管理体系，有助于促进组织不断寻求改进。

4.2 安全管理策略

安全管理策略涉及以下方面，与其他要素的关系见图 2。

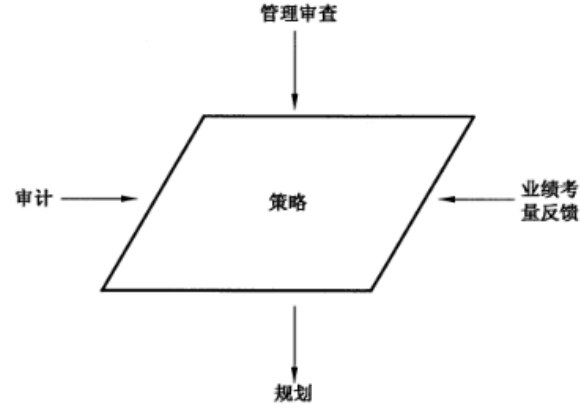

图 2 安全管理策略

a) ISO 28000 要求

组织的最高管理者应授权全面的安全管理策略。策略应符合以下要求：

a) 符合其他组织策略；

b) 提供能确保具体安全管理目标、指标和计划得以实现的框架；

c) 符合组织的总体安全威胁和风险管理框架；

d) 适用于对组织造成的威胁以及组织的运营性质和规模；

e) 明确阐述总体/全面的安全管理目标；

f) 包括对安全管理流程持续改进的承诺；

g) 包括承诺遵守当前适用法律、法规和监管要求以及组织同意的其他要求；

h) 应获得最高管理者的支持。

i) 应予以实施和维护，并形成文件；

j) 向希望获悉个人安全管理义务的相关员工和第三方(包括承包商和访客)传达；

k) 风险承担者可以获得(视情况而定)；

l) 如果出现影响安全管理体系的连续性或者相关性的对其他组织的收购或兼并或改变组织经营范围，可对其进行审查。

注：组织可选择制定详细的内部安全管理策略，以便提供充足的信息和指示，从而推动安全管理体系(部门内容可能为机密信息)，并制定包含如下信息的简述版本(非机密信息)：向利益相关方及其他相关方传播的广义目标。

b) 目的

安全策略是对最高管理者安全承诺的简要声明。安全策略确定了整体的方向感，规定了组织的行动原则，确定了适用于整个组织所要求的安全职责和业绩的安全目标。

宜将安全策略编制成文，并获得组织最高管理者的授权。

c) 典型输入

在建立安全策略时，管理层宜考虑以下项目，尤其是与其供应链有关的：

- 与组织总体业务相关的方针和目标；
- 组织过去和当前的安全绩效；
- 利益相关方的需求；
- 持续改进的机会和需求；
- 资源需求；
- 员工贡献；
- 承包商、利益相关方及其他外部人员的贡献。

d) 过程

在建立安全策略并对其进行授权时，最高管理者宜考虑以下要点。一个得以有效制定和传达的安全策略宜：

1) 与组织安全风险的性质和规模相匹配；

威胁识别、风险评估和风险管理是一个成功的安全管理体系的核心，宜体现在组织的安全策略中。

安全策略宜与组织的未来愿景一致，宜切实可行，对组织面临的风险的性质，既不夸大，也不忽视。

2) 包括持续改进的承诺；

全球安全威胁增加了组织在降低供应链事件风险方面的压力。除了履行法律、国家和监管职责及其他组织[如世界海关组织(WCO)]编制的规范和指南，组织宜以有效并高效地改进其安全绩效和安全管理体系为目标，满足不断变化的全球贸易、商业和监管需求。

尽管安全策略声明中可能包括广泛的行动范围，策划的绩效改进宜体现在安全目标(见 4.3.3)中，

并通过安全管理方案(4.3.5)进行管理。

3) 包括至少遵守当前适用的安全法规以及组织遵守的其他要求的承诺;

组织需遵守适用的安全监管要求。安全策略承诺,即组织公开承认其有义务遵守(若不超越)任何法规或其他要求,包括强制或自愿遵守的法规或要求,如世界海关组织《全球贸易安全与便利标准框架》。

注:"其他要求"指企业或集团方针、组织内部标准或规范或组织遵守的行业准则等。

4) 得以记录、实施和保持;

策划和准备是成功实施的关键。通常,因为缺乏足够和恰当的资源支持,安全策略声明和安全目标不可实行。在公开声明前,组织宜确保任何必要的资金、技能和资源可用,并确保所有安全目标在框架内部实际可行。

为了使安全策略有效,安全策略宜予以记录和定期评审以持续保持充分性,并在必要时予以修正或修订。

5) 传达给所有员工,旨在使其意识到个人安全义务;

员工的参与和承诺对确保安全至关重要。

需使员工意识到安全管理对其自身工作环境质量的影响,并宜鼓励员工积极参与安全管理。

除非员工(处于各个层级,包括管理层)理解组织的方针及其职责,并有能力执行所要求的任务,否则,其不可能对安全管理做出有效的贡献。

这就要求组织向员工明确传达其安全策略和安全目标,并提供一个框架,使其能够衡量自身的安全绩效。

6) 可供利益相关方所用;

组织的安全绩效所涉及或影响的任何个人或团体(无论内部或外部)均会对安全策略声明感兴趣。因此,宜建立一个安全策略沟通过程。必要时,该过程宜确保利益相关方收到了安全策略。

7) 予以定期评审,以确保对于组织的相关性和适宜性。

随着法律法规的发展和利益相关方期望值的增加,做出变更在所难免。组织安全策略和管理体系需予以定期评审,以确保其持续适宜性和有效性。

一旦做出变更,宜尽快沟通。

e) 典型输出

典型输出是全面、简明、易于理解的安全策略,必要时在组织内部并与利益相关方沟通。

4.3 安全风险评估和策划

安全风险评估和策划涉及以下方面,策划与其他因素的关系见图 3。

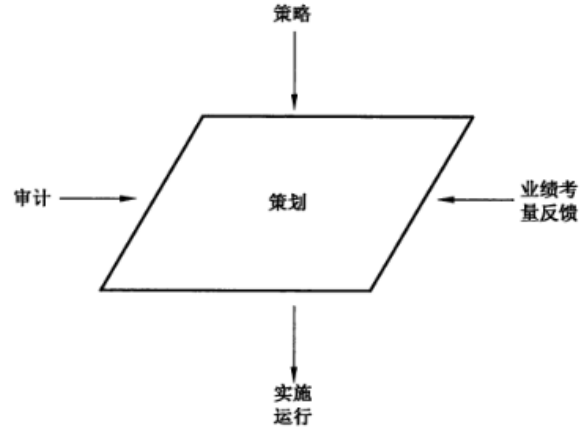

图 3 策划

4.3.1 安全风险评估

安全风险评估在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

组织应制定并维护一系列程序，以便对安全威胁、安全管理相关威胁和风险进行持续识别和评估，以及对必要管理控制措施进行识别和实施。安全威胁和风险识别、评价和控制方式应至少适合于运营的性质和规模。评估时应考虑到某事件及其所有后果的可能性，这些后果应包括：

a) 逻辑故障威胁和风险，例如功能故障、偶然损坏、恶意损坏、恐怖事件或者刑事诉讼；
b) 运营威胁和风险，包括影响组织业绩、状况或安全的安全、人为因素和其他活动的控制；
c) 可造成安全措施和设备性能降低的自然环境事件(暴雨、洪水等)；
d) 超出组织控制范围的因素，例如外部供应设备和服务的故障；
e) 利益相关者的威胁和风险，例如无法符合监管要求或损坏声誉或品牌；
f) 安全设备的设计与安装，包括更换、维护等；
g) 信息和数据管理和交流；
h) 对运营持续性造成的威胁。

组织应确保考虑到评价结果和控制效果，并在适当情况下纳入以下内容中：

a) 安全管理目标和指标；
b) 安全管理计划；
c) 确定设计、规范和安装的要求；
d) 确定适当资源(包括人员水平)；
e) 确定培训需求和技能(见 4.4.2)；
f) 制定运行控制措施(见 4.4.6)；
g) 组织的全面威胁和风险管理框架。

组织应记录上述信息，并保持更新。

组织进行威胁和风险识别与评价的方法应符合以下要求：

a) 应确定其范围、性质和时间，确保其具有主动性而非被动性；
b) 收集所有与安全威胁和风险相关的所有信息；
c) 对威胁和风险进行分类并区分可避免、消除或控制的威胁和风险；
d) 对措施进行监控，确保其有效、及时实施(见 4.5.1)。

b) 目的

在采用安全威胁识别、风险评估和风险管理过程后，组织宜在其领域内对重大安全风险、威胁和缺陷进行总体评价。

安全威胁识别、风险评估和风险管理过程及其输出宜作为整个安全体系的基础。在安全威胁识别、风险评估和风险管理过程与其他安全管理体系要素之间建立清晰明确的联系非常重要。

本文件的目的在于建立原则，组织可依据这些原则确定已有的安全威胁识别、风险评估和风险管理过程是否适用且充分。本文件的目的不在于就活动开展方式提供建议。

安全威胁识别、风险评估和风险管理过程宜使组织能够持续对安全风险进行识别、评估和控制。

在任何情况下均宜考虑组织内部正常的和异常的运行以及潜在的紧急情况。

安全威胁识别、风险评估和风险管理过程的复杂度在很大程度上取决于以下因素：组织规模、组织内部工作场所情况以及安全风险的性质、复杂度和重要性。ISO 28000:2007 中 4.3.1 的目的并非强制安全风险非常有限的小型组织进行复杂的安全威胁识别、风险评估和风险管理。

安全威胁识别、风险评估和风险管理过程宜考虑执行这三个过程所需的成本和时间以及可靠数据

的可用性。出于监管或其他目的创建的信息可用于这些过程。组织还可考虑其对所关注的安全威胁的实际控制程度。组织宜确定安全威胁的类型，同时考虑与现有和过去的相关活动、过程、产品和/或服务有关的输入与输出。

安全风险评估宜由具有资质的人员实施，采用获得认可的方法，并可形成文件。

尚未建立安全管理体系的组织可通过风险评估确定其安全风险相关的当前状况，目的在于对组织所面临的安全威胁进行考虑，并用作建立安全管理体系的基础。组织宜在初始评审时考虑下列项目(包括但不限于)：

- 法律和法规要求；
- 对组织所面临的安全威胁的识别；
- 从相应的监督和情报组织获取安全威胁和风险信息；
- 对现有的全部安全管理实践、过程和程序进行的检查；
- 对以往事件和紧急情况调查反馈进行的评价。

依据活动的性质，实施评估的适用方法包括检查表、访谈、直接检验和测量、以往管理体系审核或其他评审的结果。所有这些活动宜遵循一套文件化且可重复的方法。

需强调的是，建议通过初始评审创建一个基准，并非替代 4.3.1 中其他部分规定的结构化系统方法的实施。

c) 典型输入

典型输入包括下列项目：

- 安全法律及其他要求(见 4.3.2)；
- 安全策略(见 4.2)；
- 事件记录；
- 不符合项(见 4.5.3)；
- 安全管理体系审核结果(见 4.5.5)；
- 来自员工及其他相关方的沟通信息(见 4.4.3)；
- 来自工作场所中员工安全咨询、评审和改进活动的信息(这些活动可具有主动性或被动性)；
- 与组织相关的最佳实践和典型安全风险的信息，以及类似组织中出现的事件和紧急情况的信息；
- 行业标准；
- 政府警示；
- 有关组织设施、过程和活动的信息，包括以下内容：
  - 有关变更控制程序的详细信息；
  - 选址规划；
  - 过程手册和运行程序；
  - 安全数据；
  - 监测数据(见 4.5.1)。

d) 过程

1) 安全威胁识别、风险评估和风险管理

i) 概述

风险管理措施宜体现这样一个原则，即可行时，通过可降低事件发生的可能性或安全相关事件的潜在严重程度消除安全风险或降为可行的最低安全风险。安全威胁识别、风险评估和风险管理过程是风险管理中的主要工具。

安全威胁识别、风险评估和风险管理过程在各行业有很大的区别，范围从简单的评估到使用大量文件的复杂定量分析。组织宜策划和实施适当的安全威胁识别、风险评估和风险管理过程，符合其需求并

适用于其工作场所的情况，且有助其遵守所有的安全法律要求。

安全威胁识别、风险评估和风险管理过程宜作为主动措施而非被动措施实施，即宜在发生新的活动或修订程序之前实施。所有已确定的必要的风险降低和控制措施宜在发生变化前实施。

对于现有活动，组织宜对有关威胁识别、风险评估和风险管理的方法、人员资质、文件、数据和记录进行更新，并进行扩展以便在新进展和新活动或更改的活动发生前将其纳入考虑范围。

安全威胁识别、风险评估和风险管理过程宜不仅应用于“常规”的设施运行和程序，还宜应用于定期或临时运行/程序。

组织不仅宜考虑其自身人员活动所造成的安全风险和其他风险，还宜考虑分包商、来访人员活动以及使用其他方提供的产品或服务造成的安全风险和其他风险。

ii) 过程

安全威胁识别、风险评估和风险管理过程宜形成文件并包括以下要素：

- 对安全威胁的识别；
- 采用现有(或拟定的)控制措施对风险进行的评价(考虑具体安全威胁的暴露程度、控制措施失效的可能性以及损伤、损坏和运行连续性造成的可能的严重后果)；
- 对当前和剩余风险可接受程度的评价；
- 对所需的附加风险管理措施的识别；
- 评估风险管理措施是否足以将风险降低到可接受水平。

此外，过程还宜包括以下内容：

——将要采用的任何形式的安全威胁识别、风险评价和风险管理的性质、时效、范围和方法；

——适用的安全法规或其他要求；

——负责执行这些过程的人员的职责和权限；

——过程执行人员的能力要求和培训需求(见 4.4.2)(取决于所采用过程的性质或类型，组织可能还有必要采用外部建议或服务)；

——员工安全输入数据、评审和改进活动的信息的使用(这些活动可具有主动性或被动性)；

iii) 后续措施

在执行安全威胁识别、风险评估和风险管理过程之后：

——宜提供清晰证明，对被确定有必要采取的所有纠正或预防措施(见 4.5.2)予以监视，以便按时完成(这可能要求实施进一步的安全威胁识别和风险评估，以反映拟定的对风险管理措施的变更和确定修改的残余风险的估算)；

——宜将纠正或预防措施的结果和完成的进度反馈给管理层，作为管理评审(见 4.6)的输入和用于确立修订的或新的安全目标；

——组织宜确定执行具体安全任务的人员的能力是否符合在建立必要的风险管理时风险评估过程规定的能力；

——适用时，后续运行经验反馈宜用于修正过程或作为过程的基础的数据。

2) 在完成安全威胁识别、风险评估和风险管理初步评价之后(见 4.6)

宜在安全策略文件中规定的预定时间或期限内，或在管理层预定的时间内对安全威胁识别、风险评估和风险管理过程进行评审，该评审可构成管理评审过程(见 4.6)的一部分。这一期限可能依据以下因素的变化而变化：

- 安全威胁的性质；
- 风险的严重程度；
- 正常运行的变更。

当组织内部发生的变更导致对现有评估的有效性产生怀疑时，宜进行评审。此类变更包括以下要素：

- 设施或供应链的扩增、缩减、改组和变更；
- 职责的重新分配；
- 外源性安全威胁工作方法或行为模式的变更。

e) 典型输出

以下要素宜形成文件化程序：

- 安全威胁的识别；
- 已确定的安全威胁相关的风险的确定；
- 各类安全威胁相关的风险的等级指示，及风险是否可接受；
- 有关风险(尤其是不能接受的风险)监视和控制措施(见 4.4.6 和 4.5.1)的说明或索引；
- 适当时，安全目标和降低已识别的风险(见 4.3.3)的措施及监视风险降低过程的任何后续活动；
- 对实施控制措施的能力和培训要求的识别(见 4.4.2)；
- 作为体系的运行控制要素一部分的必要控制措施(4.4.6)；
- 上述各项程序产生的记录。

4.3.2 法律、法规及其他安全监管要求

法律、法规及其他安全监管要求在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织应制定、实施并维护满足以下要求的程序：
>
> a) 确定并使用适用的法律要求及组织采用的有关安全威胁和风险的其他要求；
>
> b) 确定这些要求应用于安全威胁和风险的方式。
>
> 组织应及时更新这些信息。应向员工及其他相关第三方(承包商)传达有关法律及其他要求的相关信息。

b) 目的

组织需意识到并了解适用法律及其他要求对其活动产生的或将产生的影响以及将这些信息传达给相关人员的方式。

ISO 28000:2007 的 4.3.2 旨在提高对法律和监管职责的意识和了解。其目的不在于要求组织针对极少参考或使用的法律或其他文件建立文件库。

c) 典型输入

典型输入包括下列项目：

- 组织供应链的详细资料；
- 安全威胁识别、风险评估和风险管理结果(见 4.3.1)；
- 最佳实践(如规范、行业协会指南)；
- 法律要求及政府、政府间、贸易协会规范、实践与法规；
- 信息来源清单；
- 国家、区域或国际标准；
- 组织内部要求；
- 利益相关方要求；
- 供应链动态管理过程。

d) 过程

宜识别相关法规及其他要求。组织确定获取信息的最恰当方法，包括支持信息的媒介(如纸质、光盘、磁盘或互联网)。组织还宜评价适用的要求、要求适用的情况以及需接受信息的主体。

e) 典型输出

典型输出包括下列项目：

- 识别和获取信息并不断更新的程序；
- 识别适用的要求及其适用的情况(可采用登记表的形式)；
- 可在组织所确定的场所获得的要求(适用情况下的真实文本、总结或分析)；
- 监视新安全法规下对控制措施实施情况的程序。

4.3.3 安全管理目标

安全管理目标在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织应在内部在相关职能和层面上制定、实施和维护文件化安全管理目标。这些目标应该源于并符合本策略。在制定并审查其安全管理目标时，组织应考虑以下问题：
>
> a) 法律、法规及其他安全监管要求；
>
> b) 相关的安全威胁和风险；
>
> c) 技术及其他方案；
>
> d) 财务、运营和业务要求；
>
> e) 风险承担者的观点。
>
> 安全管理目标应满足下列要求：
>
> a) 与组织的持续改进承诺一致；
>
> b) 应进行量化(若可行)；
>
> c) 传达给所有相关人员及第三方，包括希望获悉其自身义务的承包商；
>
> d) 定期审查，以确保与安全管理策略的相关性和一致性。必要时，应对上述目标进行相应修改。

b) 目的

需确保在整个组织内(可行时)所建立的可测量的安全目标与安全策略相一致。

c) 典型输入

典型输入包括下列项目：

- 与组织总体业务相关的方针和目标；
- 安全策略，包括持续改进承诺(见 4.2)；
- 安全威胁识别、风险评估和风险管理的结果(见 4.3.1)；
- 法律及其他要求(见 4.3.2)；
- 技术选择方案；
- 财务、运营和业务要求；
- 员工及利益相关方关注(见 4.4.3)；
- 工作场所中员工安全输入、评价和改进活动信息(这些活动可具有主动性或被动性)；
- 对建立的安全目标进行的分析；
- 有关安全不符合项、事件与财产损失的以往记录；
- 管理评审结果(见 4.6)。

d) 过程

通过利用输入的信息或数据，相应的管理层宜识别、建立并优先考虑安全目标。

在安全目标建立期间，宜特别注意有关最可能受个人安全目标影响的人员的信息或资料，这样有助于确保指标合理且被更广泛地接受。考虑来自组织以外(例如，承包商、供应商、业务伙伴、治安和情报组织或利益相关方)的信息或资料也是有用的。

相应级别的管理层宜定期就安全目标的建立召开会议。对于某些组织，可能需要记录建立安全目标的过程。

安全目标宜包括广泛的企业安全问题以及组织内供应链、个别职能和各层次的具体安全问题。

可行时，宜就各安全目标确定适合的指标。这些指标宜用于监视安全目标的实施。

安全目标宜合理且可实现，以便组织能实现这些目标并监视实现过程。为实现各安全目标，宜确定合理且可实现的时间范围。

根据组织规模、安全目标的复杂性和时间范围，安全目标可分成单独的目标。不同层次的目标和安全目标之间宜有明确联系。

安全目标类型示例包括：

- 降低风险水平；
- 引进安全管理体系附加特性；
- 改进现有设施所采取的措施；
- 杜绝特殊意外事件或降低发生的频率。

宜(通过培训或小组简报会议；见 4.4.2)向相关人员沟通安全目标并按安全管理计划(见 4.3.4)开展部署。

e) 典型输出

典型输出包括组织内部各职能记录的、可测量(如可行)的安全目标。

4.3.4 安全管理指标

安全管理指标在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织宜制定、实施并记录适合其需要的安全管理指标。上述指标不仅宜根据安全管理目标制定，而且宜与安全管理目标一致。
>
> 指标宜：
>
> a) 细节层次适当；
>
> b) 符合具体性、衡量性、可达性、相关性和时限性(若可行)原则；
>
> c) 传达给所有相关人员及第三方，包括希望获悉其自身义务的承包商；
>
> d) 定期审查，以确保与安全管理目标的相关性和一致性。必要时，宜对上述指标进行相应修改。

b) 目的

设定安全指标以在规定时间框架内实现目标。

c) 典型输入

典型输入包括下列项目：

- 与组织整体业务相关的方针和目标；
- 安全策略，包括对持续改进的承诺(见 4.2)；
- 安全威胁识别、风险评估和风险管理的结果(见 4.3.1)；
- 法律及其他要求(见 4.3.2)；
- 技术选择方案；
- 财务、运行和业务要求；
- 员工和利益相关方的关注(见 4.4.3)；
- 工作场所中的员工安全输入、评估和改进活动相关信息(这些活动可具有主动性或被动性)；
- 对建立的安全目标的分析；
- 有关安全不符合项和事件的以往记录；

- 管理评审的结果(见 4.6)。

d) 过程

在安全方案中确定过程,该过程为旨在满足目的的可实现的目标。

通过利用输入的信息或数据,相应的管理层宜识别、建立并优先考虑安全指标。指标宜具备具体性、时限性和可测量性。

在安全指标建立期间,宜特别注意有关最可能受个人安全指标影响的人员的信息或数据,这样有助于确保指标合理且被更广泛地接受。考虑来自组织以外(例如,承包商、供应商、业务伙伴、治安和情报组织或利益相关方)来源的信息或数据也是有用的。

修改安全目标之后,宜对相应级别的管理层宜就建立安全指标召开的会议进行评审。对于某些组织,可能需要记录建立安全指标的过程。

安全指标宜解决广泛的企业安全问题以及组织内供应链、个人职能和各层次的具体安全问题。

宜就各安全指标确定适合的具体指标。这些具体指标宜用于监视安全指标的实施。

安全指标宜合理且可实现,以便组织能实现这些目标并监视实现过程。为实现各安全指标,宜确定合理且可实现的时间范围。

根据组织规模、安全指标的复杂性和时间范围,安全指标可分成单独的指标。不同层次的目标和安全指标之间宜有明确联系。

典型的安全指标示例包括:

- 在规定时间框架内降低风险水平;
- 引进新技术降低风险或减轻来自安全威胁的冲击;
- 采取措施改进现有设施及其时间范围;
- 杜绝特殊意外事件或降低发生的频率。

宜(通过培训或小组简报会议;见 4.4.2)向相关人员沟通安全指标并按安全管理计划(见 4.3.4)开展部署。

e) 典型输出

典型输出包括为组织内部各职能记录的、可测量的(如可行)安全指标。

4.3.5 安全管理方案

安全管理方案在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织宜制定并实施安全管理计划,以实现其各项目标和指标。
>
> 上述计划宜在优化后予以优先考虑;同时,组织宜确保上述计划得以经济、高效地实施。
>
> 安全管理计划宜包括满足下列要求的文件:
>
> a) 规定了实现各项安全管理目标和指标的职责和权力;
>
> b) 规定了实现各项安全管理目标和指标的手段和时标。
>
> 宜对各项安全管理计划进行定期审查,以确保其有效,且符合各项目标和指标。必要时,宜对上述计划进行相应修改。

b) 目的

安全管理方案宜与目标和指标存在直接联系。各管理方案宜说明组织如何将目标和方针承诺转化为实际行动并实现安全目标和指标。方案要求就所采取的行动制定策略和计划,宜记录和沟通这一制定过程。宜监视、评审和记录方案与满足所述目标的进展情况。方案的遏制和缓和策略宜基于安全管理威胁和危害识别及风险评估的结果(如:影响分析、方案评估、运行经验)。

c) 典型输入

典型输入包括下列项目:

- 安全目标和指标；
- 法律及其他要求；
- 安全威胁识别、风险评估和风险管理的结果；
- 组织运行的详情情况；
- 工作场所中员工安全输入、评审和改进活动(这些活动可具有主动性或被动性)的相关信息；
- 对新的或不同的技术选择方案所提供的机会的评审；
- 持续改进活动；
- 实现组织安全目标所需资源的可获得性。

d) 过程

安全管理方案宜确定：

- 实现目标的职责；
- 实现目标的手段；
- 实现目标的时间范围。

方案宜考虑通过方法论的和科技性的方案，以及其他实体的经验减轻威胁，同时考虑财务会计、运行和业务要求以及合作组织和利益相关方的意见。

宜为各任务分配适当的职责和权限，并对各单项任务安排时间范围，以满足相关安全目标的总时间范围。还宜为各任务分配适宜的资源(如财务、人力、设备、物流)。

如工作实践、过程、设备或设施出现重大变动或更改时，方案宜考虑新的安全威胁识别和风险评估演练。安全管理方案宜考虑就预期的变更向相关人员进行咨询。

e) 典型输出

典型输出包括为实现 4.3.3 和 4.3.4 中所述目标和指标所确定和记录的安全管理方案。

4.4 实施和运行

实施和运行涉及以下方面，实施和运行与其他要素的关系见图 4。

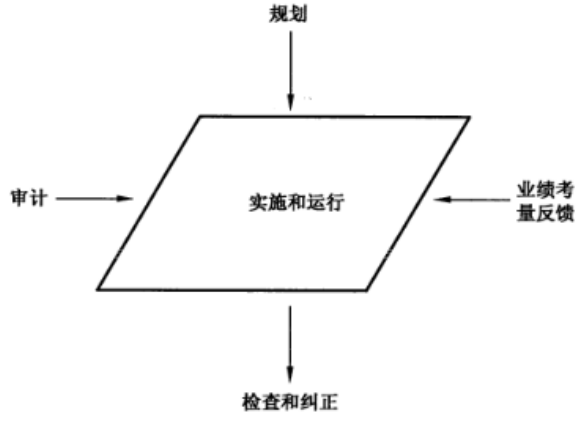

图 4 实施和运行

4.4.1 安全管理结构、权限和职责

安全管理结构、权限和职责在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

组织宜确立一个有关作用、职责和权力的组织，并符合其安全管理策略及各项目标、指标和计划的要求。

同时，这些作用、职责和权力宜予以规定、记录，并传达给负责实施和维护工作的相关人员。

最高管理者宜通过以下方式说明其在安全管理体系（过程）制定和实施方面以及不断增强有效性方面的承诺：

a) 指定最高管理者内某成员（无论是否有其他职责）负责组织安全管理体系的总体设计、维护、记录和改善工作；

b) 向管理层内某成员授予必要权力，以确保各项目标和指标得以实施；

c) 确定和监测组织利益相关者是否符合要求和预期目标，并及时采取适当措施实现这些预期目标；

d) 确保能够获取足够的资源；

e) 考虑到安全管理策略及各项目标、指标和计划等可能对组织的其他方面产生的不利影响；

f) 确保组织其他部门制定的任何安全计划均能够对安全管理体系进行互补；

g) 向组织传达满足其安全管理要求以符合其策略的重要性；

h) 确保对安全相关威胁和风险进行评价，并根据具体情况将其纳入组织威胁和风险评价范围内；

i) 确保安全管理目标、指标和计划的可行性。

b) 目的

为促进有效安全管理，有必要确定、记录和沟通角色、职责和权限。宜仅派了解安全的人员（见第3章定义）执行关键安全任务。为确保执行安全任务，宜提供充分资源。

c) 典型输入

典型的输入包括下列内容：

- 组织结构；
- 安全风险识别、风险评估和风险控制结果；
- 安全目标、指标和方案；
- 法律及其他要求；
- 工作说明；
- 需要和/或已接受安全审查的合格安全人员名单。

d) 过程

1)概述

全体人员履行义务是安全管理体系的一部分，宜确定职责和权限，包括对不同职能间对接的职责的明确界定。

上述界定适用于以下人员：

- 最高管理者；
- 组织的各级管理人员；
- 负责接待可进入场所和接触员工的承包商和来访者的人员；
- 安全培训负责人员；
- 对安全至关重要的设备和运行的负责人员；
- 组织内经安全审查的员工或其他安全专家；
- 负责协商论坛的员工安全代表。

然而，组织宜沟通并宣传这一观念，即安全是组织中每个人的责任，不仅仅是负有明确的安全管理体系义务的责任人员的职责。

2) 明确最高管理者的职责

最高管理者的职责宜包括确定组织的安全策略并确保实施安全管理体系。作为承诺的一部分，最高管理者宜委任和指定专门的管理者代表，赋予其实施安全管理体系的职责和权限。（对于庞大或复杂的组织，可能有不止一名委任代表。）

3) 明确安全管理者代表的职责

安全管理代表宜具有确保实施和记录安全管理体系、持续接触最高管理者、得到被授权监视安全职能整体运行情况的其他人员的支持的职责和权限。管理者代表宜定期了解体系运行状况，并宜积极参与定期评审和设定安全目标。宜确保分配给这些人员的其他义务或职能与其安全职责不冲突。

4) 明确各级管理者的职责

各级管理者的职责包括对其运营场所进行安全管理。其首要责任在于各级管理者宜恰当地确定组织内所有安全专家职位的角色和职责，以避免对角色和职责的混淆。这宜包括通过上升至较高管理层解决安全问题与生产力因素之间的任何冲突所做的安排。

5) 角色和职责的文件化

安全职责和权限宜以适合组织的形式形成文件。可采取以下一种或多种形式或组织选用的其他形式：

- 安全管理体系手册；
- 工作程序和任务说明；
- 工作说明；
- 入门培训成套方案和理念培训方案。

如果组织选择发布包含员工角色和职责以外的书面工作说明，安全职责宜包含于该工作说明中。

6) 角色和职责的沟通

安全职责和权限宜适当地向组织内相关人员沟通。这宜确保个人理解范围、不同职能间的对接以及发起行动的途径。

7)资源

管理层宜确保为供应链安全提供充足资源，包括设备、人力资源、专业知识和培训。

只要资源足以执行安全方案和活动，包括绩效测量和监视，即可认为资源是充足的。

对于已建立安全管理体系的组织，可至少通过以实际结果对比预期成果的形式在一定程度上评价资源充足性。

8) 管理者的承诺

管理者宜提供其对安全承诺的明显证明。证明手段可包括巡视和检查现场、参与安全事件调查和为纠正措施提供资源、出席安全会议及发出支持信息。

e) 典型输出

典型输出包括下列内容：

对所有相关人员的安全职责和权限的界定；

手册、程序、培训文件包中有关角色或职责的记录；

将角色和职责传达给所有员工和其他利益相关方的过程；

各级管理者的积极参与和对安全的支持。

4.4.2 能力、培训和意识

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

组织宜确保负责安全设备和工艺设计、操作和管理的人员有相应资格和经验且经过适当培训。同时，组织宜制定并贯彻相关程序，以使其工作人员或代表意识到：

a) 遵守安全管理策略和程序以及符合安全管理体系要求的重要性；

b) 在遵循安全管理策略和程序及安全管理体系要求(包括应急准备和响应要求)期间的作用和职责；

c) 违背规定操作程序对组织安全造成的潜在后果。

宜对胜任能力和培训情况予以记录。

b) 目的

组织宜制定有效程序，确保人员能执行所指定的安全职能并意识到安全风险。

c) 典型输入

典型输入包括以下项目：

- 确定角色和职责；
- 工作说明(包括拟执行的安全任务详情)；
- 员工业绩评估；
- 安全风险识别、风险评估和风险控制结果；
- 程序和运行说明；
- 安全策略和安全目标；
- 安全方案。

d) 过程

下列要素宜包括于过程中：

- 对组织内部各级和各职能所需的安全意识和能力的系统识别；
- 为识别并补救个人当前所具备水平和所需安全意识与能力水平之间的差异所做的安排；
- 提供及时且系统的必要培训；
- 评价个人，确保其获得并保持所需的知识和能力；
- 维护适当的个人培训和能力记录。

注：特别强调的是整个组织的安全意识对成功的安全管理体系及其有效实施至关重要。

宜建立和维护安全意识和培训方案，包含下列领域：

- 对安全风险和威胁的不断认识；
- 对组织的安全布置和个人具体角色和职责的理解；
- 针对员工和组织内部不同分公司、场所、部门、区域、工作或任务间调转的人员的上岗和持续培训的系统方案；
- 本部门安全布置和安全风险、风险、防范措施和需遵循程序的相关培训，宜在工作开始前提供；
- 有关实施安全风险识别、风险评估和风险控制的培训(见 4.3.1d)；
- 在安全体系中有特定角色的员工所需的特定内部或外部培训，包括员工安全代表；
- 针对管理员工、承包商和其他人(如临时工)的人员的各自安全职责的培训。确保这些人员及在其管理下工作的人员了解安全威胁和运行风险，无论何处发生威胁和风险。另外，也能确保通过遵循安全程序，人员具备安全实施活动的必要能力；
- 最高管理者在确保安全管理体系职能以控制风险和减少弊端、伤害和对组织造成的其他损失

方面的角色和职责(包括组织和个人的法律责任);

- 根据所面临的风险水平,针对承包商、临时工和来访人员的培训和意识方案。

宜评价培训和意识方案的有效性。这可能涉及评估,作为培训活动和/或相应的现场检查的一部分,以确定这些人员是否获得能力和充足的意识,或监视培训带来的长期影响。

e) 典型输出

典型输出包括下列项目:

- 针对个人角色的能力要求;
- 培训需求的分析;
- 培训方案/计划;
- 组织内部可提供的培训课程/产品的范围;
- 培训记录和培训有效性评价记录;
- 安全意识方案;
- 安全意识评价。

4.4.3 沟通

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

组织宜制定有相关程序,以确保向或从相关员工、承包商及其他利益相关者处传达相关安全管理信息。 由于某些安全相关信息具有敏感性,因此宜在传播之前适当考虑到信息的敏感性。

b) 目的

组织宜通过咨询和沟通的过程鼓励受运行影响的相关人员参与良好安全实践和支持安全策略和安全目标。

c) 典型输入

典型输入包括下列项目:

- 安全策略和安全目标;
- 相关的安全管理体系文件;
- 安全风险识别、风险评估和风险控制程序;
- 安全角色和职责的确定;
- 正式和非正式的员工与管理层安全协商的结果;
- 培训方案详情;
- 来自外部的相关信息。

d) 过程

组织宜记录并促进安排,通过这样的安排组织与员工和其他相关方(如承包商、来访人员、利益相关方、业务伙伴、政府)协商,并与其沟通有关的安全信息。

宜包括员工参与下列过程的安排:

- 就方针的制定和评审、安全目标和风险管理过程和程序的实施的决策的制定和评审的协商,包括实施与自身活动相关的安全风险评估和风险控制;
- 就影响工作场所安全的变更的协商,如引进新的或调整设备、设施、化学品、技术、过程、程序或

工作模式；

宜鼓励员工对安全事务表达意见，并使其知晓详细的安全命令管理链。

e) 典型输出

典型输出包括下列内容：

- 通过安全委员会或类似组织与管理层和员工进行协商；
- 员工参与安全风险识别、风险评估和风险控制；
- 积极鼓励员工进行安全协商、评审和改进工作场所中的活动，并反馈至安全问题管理人员；
- 具备明确角色的员工安全代表和与管理层沟通的机制，包括，例如，参与意外事故和事件调查、现场安全巡视等；
- 对员工和其他利益方(如承包商或来访人员)的安全介绍；
- 包含安全信息的告示板；
- 安全简讯；
- 安全海报方案；
- 与相应政府组织及供应链伙伴分享敏感安全信息的其他手段。

4.4.4 文件

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织宜制定并贯彻安全管理文件系统，该系统包括但不限于以下内容：
> a) 安全策略、目标和指标；
> b) 安全管理体系的范围说明；
> c) 安全管理体系的主要部分及其与相关文件的相互关系和引用关系；
> d) 本国际标准中规定的记录等文件；
> e) 组织为了确保对与其重大安全威胁和风险相关的过程进行有效地规划、操作和控制而确定的记录等文件。
> 组织宜确定信息的安全敏感性，并宜采取措施防止在未经批准的情况进行使用。

b) 目的

组织宜记录并维护最新文档以确保其安全管理体系得到了解和有效地实施和运行。

c) 典型输入

典型输入包括下列项目：

- 组织为支持安全管理体系和安全活动并履行 ISO 28000 的要求制定的文档和信息系统的详情；
- 职责和权限；
- 有关承载文档或信息的设施和限定条件的信息，其中限定条件为可呈现文档的物理性质或使用电子或其他媒介。

d) 过程

在制定支持组织安全过程和安全管理体系必需的文档前，组织宜识别信息安全管理体系所需的数据和信息。

不要求将文档制成 ISO 28000 规定的特定格式，也不要求必须替换现有文档，如手册、程序或工作说明等(如已充分描述了当前的安排)。如组织已建立安全管理体系并形成文件，则可证明组织能更方

便和有效地制定描述现有程序与 ISO 28000 要求的相互关系的交叉参考文件。

宜对下列内容予以考虑：

- 文档和信息使用者的职责和权限，因为这宜决定宜施加的安全程度和可用性；
- 文本文档使用的方法和环境。同样宜考虑有关信息系统电子设备的使用。

e) 典型输出

典型输出包括下列项目：

- 安全管理体系文档概述文件；
- 文件登记表、总清单或索引；
- 程序；
- 工作说明。

4.4.5 文件和数据控制

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织宜制定用于控制本国际标准第 4 章中规定的所有文件、资料和信息的各种程序，以确保：
> a) 只有授权个人才可找到并使用这些文件、资料和信息；
> b) 定期对这些文件、资料和信息进行审查，必要时进行修订，且其充分性宜获得授权人员的批准；
> c) 能够在进行安全管理体系有效运行所需操作的所有地点获取现行相关文件、资料和信息；
> d) 及时从所有发行地点和使用地点处移除作废文件、资料和信息，或者以其他方式避免非预期使用；
> e) 为法律或/和知识保护所保存的所有档案文件、资料和信息予以适当标识；
> f) 这些文件、资料和信息的安全性、电子备份充裕度和恢复性。

b) 目的

宜识别和控制包含了安全管理体系和组织安全活动绩效的信息的所有文件和数据。

c) 典型输入

典型输入包括下列项目：

- 组织为支持安全管理体系和安全活动并履行 ISO 28000 的要求制定的文档和信息系统的详情；
- 职责和权限详情。

d) 过程

书面程序宜确定对安全文件的识别、批准、发布、访问及清除的控制，及对数据安全的控制。这些程序宜清晰界定所应用的文档和数据类别，以及基于安全敏感性的分级层次。

必要时，文档和数据宜供经授权的人员使用，无论在常规还是非常规条件下，包括紧急情况下。

e) 典型输出

典型输出包括下列项目：

- 文件控制程序，包括指定的职责和权限；
- 文件登记表、总清单和索引；
- 受控文件及其位置的清单；
- 档案记录。

4.4.6 运行控制

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织宜确定满足下列要求所需的各项运作和活动：
>
> a) 安全管理策略；
>
> b) 控制具有重大风险的各项活动和减轻具有重大风险的各项威胁；
>
> c) 遵守法律、法规及其他安全监管要求；
>
> d) 安全管理目标；
>
> e) 安全管理计划交付；
>
> f) 供应链达到规定安全程度。
>
> 组织宜确保能够通过下列方式在特定条件下进行这些运作和活动：
>
> a) 制定并贯彻实施书面控制程序，以防止出现导致 4.4.6a)～f)中所列明运作和活动无法实现的情况；
>
> b) 对从上游供应链活动产生的任何威胁进行评价，控制并降低对组织及其他下游供应链操作人员的影响；
>
> c) 针对影响安全的商品服务制定并实施相关要求，并告知各供应商和供应商。
>
> 这些程序中宜包括针对设备和仪表等(根据具体情况)有关安全项目的设计、安装、运行、改造和改良工作的控制情况。在改进现有布局或引入新布局时，如果可能会对安全管理运作和活动产生影响，则组织宜在实施之前考虑到相关安全威胁和风险。有待考虑的新型或改进后布局宜包括：
>
> a) 改进后组织结构、作用或职责；
>
> b) 改进后安全管理策略、目标、指标或计划；
>
> c) 改进后过程和程序；
>
> d) 引入新型基础设施和安全设备或技术(可包括软件和/或硬件)；
>
> e) 根据具体情况引入新承包商、供应商或人员。

b) 目的

无论是要求控制运行安全风险、完成安全策略和目标，还是在实现安全指标和符合法律及其他要求，组织均宜建立和维护安排以确保有效利用控制及应对措施。

c) 典型输入

典型输入包括下列项目：

- 安全策略和安全目标；
- 安全威胁识别和风险评估结果；
- 识别的法律、法规和其他要求。

d) 过程

组织宜建立程序控制其识别的风险(包括由承包商、其他供应链业务伙伴或来访人员带来的风险)，并编成案例，即若未控制风险，可能导致发生事件、突发事件或其他偏离安全策略和安全目标的情况。宜定期评审风险管理程序，确保适宜性和有效性，并宜实施已识别出的必要变更。

若风险危及顾客或其他外方的场所或供应链其他部分的控制区域，程序宜对此类情况加以考虑；例如员工在顾客的场所工作。有时需要与外方就该种情况下的安全进行协商。

通常产生风险的区域和针对风险采取的控制措施举例如下：

1） 采购或转让商品和服务以及外部资源的使用权

包括如下项目：

- 评价和定期再评价承包商的安全能力；
- 批准对新的厂房或设备设计安全措施。

2） 安全敏感任务

包括如下项目：

- 安全敏感任务的识别；
- 安全工作方法的预先确定和批准；
- 安全敏感任务人员资质的预先评定；
- 安全敏感区域人员进入控制程序。

3） 安全设备的维护

包括下列内容：

- 隔离和访问控制；
- 安全相关的设备和高集成系统的检查和测试。

e） 典型输出

典型输出包括下列项目：

- 程序；
- 运行和维护说明。

4.4.7 应急准备、响应和安全恢复

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a） ISO 28000 要求

组织宜建立并贯彻实施适当的计划和程序，以确定安全事件和紧急情况的潜在可能性及对策，并预防和减轻可能与其相关的后果。计划和程序中宜包括有关在事件或紧急情况期间或之后所需标识设备、设施或服务的提供和维护信息。 组织宜定期审查其应急准备、响应和安全恢复计划和程序的有效性，特别是发生在由安全漏洞和威胁所引起的事件或紧急情况之后。可行时，组织宜定期对这些程序进行测试。

b） 目的

本节包括安全事件发生后的预案、响应和恢复。应急准备这一术语指的是在意外安全事件或危机发生后实施的计划、准备和预防措施。

组织宜积极就通过安全威胁和风险评估过程（见 4.3.1）识别的潜在安全事件评估潜在事件和响应需要。宜制定响应计划、程序和过程，以应对潜在安全事件、测试拟定的响应措施和寻求改进响应措施的有效性。

c） 典型输入

典型输入包括下列项目：

- 安全威胁识别和风险评估；
- 本地应急服务组织和安全组织的可用性和有关经确定的任何应急响应或协商安排的详情。
- 监管、法律或其他要求；

- 以往经历和对以往事件和紧急情况以及后续行动结果的评审；
- 组织有关以往事件和紧急情况的类似经历(经验、最佳实践)；
- 治安、情报和急救员输入；
- 对所实施的行动、演习和训练的评审。

d) 过程

组织宜制定应急计划，确认和提供适当的应急安排，并通过实战训练定期测试其能力。应急准备、响应和安全恢复计划宜包括恢复安全、保护数据和设施以及确保安全连续性的措施。

实战演练宜测试安全响应计划最关键部分的有效性和应急策划过程的完整性。尽管桌面演练在策划过程中有所作用，也宜实施实战演练和训练，评价实战演练的结果，同时进行必要的变更。

具体过程包括以下内容：

1) 应急响应和安全恢复计划

当出现具体情况时，应急响应和安全恢复计划宜规定要采取的措施，包括下列内容：

- 对潜在事件和紧急情况的识别；
- 紧急情况下负责人的确定；
- 紧急情况下人员所采取措施的详情，包括现场的外部人员所采取的措施，如承包商或来访人员(如被要求转移到规定疏散点集合的人员)；
- 在紧急情况下，具有特定角色的人员的职责、权限和义务(如保安、消防员、急救人员、放射泄露/毒物污染专家)；
- 疏散程序；
- 描述安全措施和安全条件如何在短期和中期内得以恢复的程序；
- 安全材料、记录、数据和设备以及所需的应急措施的确定、定位和保护；
- 与应急服务和急救人员的对接；
- 与利益相关方的沟通；
- 紧急情况下必要信息的可用性，如工厂布局图、安全数据、程序、工作说明和联系电话；
- 与其他供应链业务/贸易伙伴的对接和沟通；
- 确保沟通系统的完整。

外部组织参与应急规划和响应予以明确记录。宜通知这些组织其参与时可能涉及的状况，并提供其所需的此类信息，以促进参与响应活动。

2) 安全设备

宜确定安全设备需求并提供充足设备，在规定时间内对此进行检验以保证持续运行。

3) 实战演练和演习

宜按照事先确定的日程进行实战演练和演习。适当且可行时，宜鼓励外部安全服务组织参与实战演练。

e) 典型输出

典型输出包括下列内容：

- 文件化的应急响应和安全恢复计划及程序；
- 安全设备清单；
- 安全设备的测试记录；
- 实战演练和演习；
- 对实战演练和演习的评审；
- 评审产生的建议措施；
- 建议措施的完成情况；
- 已完成的措施。

4.5 检查和纠正措施

检查和纠正措施涉及以下方面，与其他要素的关系见图5。

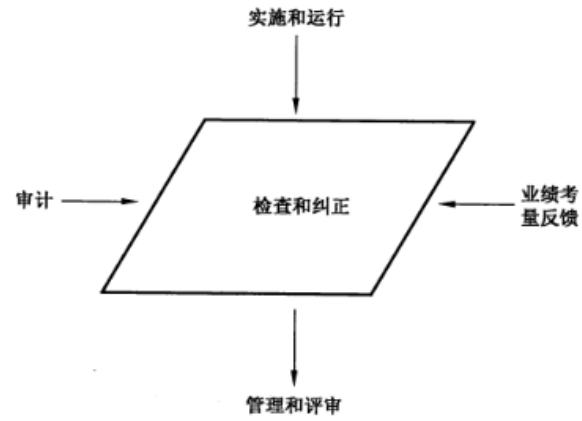

图5 检查和纠正措施

4.5.1 安全绩效测量和监视

在ISO 28000中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000要求

组织宜制定并贯彻相关程序，以便对安全管理体系的性能及安全业绩进行监测。同时，在确定关键性能参数的监测频率时，组织宜考虑到相关安全威胁和风险，包括潜在恶化机制及其后果。这些程序宜对如下内容予以规定：

a) 满足组织需求的定性和定量测定；
b) 满足组织安全管理策略、目标和指标要求的监测范围；
c) 监测是否遵守安全管理计划、运行控制标准、适用法律法规及其他安全监管要求时的主动措施；
d) 监测以下安全相关情况的被动措施：恶化、故障、事件、不符合项(包括漏报和虚假警报)及其他表明安全管理体系性能有缺陷的历史证明；
e) 足以推进随后进行纠正和预防行为分析的记录资料及监测结果。如果性能和/或测量和监测工作需要监测设备，则组织宜要求制定并贯彻设备校准和维护程序。此外，宜按照法律法规和组织策略规定的时间，保存校准、维护活动和结果记录。

b) 目的

组织宜确定整个组织及其控制或影响的供应链的安全绩效的关键绩效指标。

宜包括但不限于确定衡量以下内容的指标：

- 是否实现安全策略和安全目标；
- 是否控制和/或减轻威胁，同时有效地实施了恰当的应对措施；
- 是否从安全管理体系失效中获得经验，包括安全事件和未遂事件；
- 员工和利益相关方的意识、培训、沟通和协商方案是否有效；
- 是否创建和使用能够用于评审和改进安全管理体系的信息。

c) 典型输入

典型输入包括下列内容：

- 安全威胁识别、风险评估和风险管理(见 4.3.1);
- 法律要求、法规、最佳实践(如有);
- 安全策略和安全目标;
- 处理不符合项的程序;
- (包括与承包商相关的)安全设备测试和校准记录;
- (包括与承包商相关的)培训记录;
- 管理报告。

d) 过程

下列要素宜包括于过程中:

1) 主动和被动监视

组织的供应链安全管理体系宜包含如下的主动和被动监视:

- 宜采用主动监视检查与组织安全活动的一致性,如监视安全巡视的频次和有效性;
- 宜采用被动监视调查、分析和记录安全管理体系失效—包括紧急情况和安全事件。

主动和被动监视数据通常用于确定安全目标是否实现。

2) 测量方法/技巧

以下是一些可用于测量安全绩效的方法示例:

- 安全风险识别、风险评估和风险控制过程的结果,如是否符合世界海关组织《全球贸易安全与便利标准框架》和美国打击恐怖主义海关-贸易伙伴关系(C-TPAT)以及《欧盟授权经济经营者(AEO)条例》;
- 使用核查表进行的系统性检查;
- 安全检查;
- 评价新型供应链物流体系;
- 评审和评价物流统计模式;
- 检查安全设备以确保状态良好;
- 使用具有安全经验或正式资质的人员的可行性和有效性;
- 行为抽样:评估工作人员行为以便识别需要纠正的不良安全实践;
- 文件和记录分析;
- 其他组织中的良好安全实践衡量基准;
- 采用调查判断员工态度以查明可疑行为;
- 利益相关方的反馈。

组织需要基于风险水平决定监视的内容及频次(见 4.3.1)。宜制定基于安全威胁识别和风险评估结果、法律和法规的检查时间表,作为安全管理体系的一部分。

经授权的人员宜根据监视方案文件对过程、物流节点、业务伙伴、供应链活动和实践进行常规安全监视,该人员还宜负责关键任务的抽查,确保符合安全程序和实践规范要求。可使用核查表协助进行系统的检查和监视。

3) 安全设备

宜列出、单独识别并控制用于监视和确保安全的安全设备(如摄像头、栅栏、门、警报器等)。宜知晓设备的精确度。必要时,提供书面程序说明如何进行安全测量。宜采用恰当的方法维护安全设备,以便需要时可以使用。

需要时,制定并执行安全设备校准和维护方案。该方案宜包括以下内容:

- 校准和维护频次;

- 引用测试方法(如适用);
- 校准设备的特性;
- 规定的安全设备发生校准故障时所采取的措施。

校准和维护宜在合适条件下进行。宜制定严重或困难情况下的校准程序。

校准设备宜符合国家标准(如有)。若无此类国家标准,宜记录所采用标准的依据。

保存所有校准、维护活动和结果的记录。记录宜包含调整前后的测量详情。

宜确保用户可以清楚识别安全设备的校准状况。

不宜使用校准或维护状况不明、或发生校准故障的安全设备。另外,宜移走这些设备,并清楚标识、贴标签或其他标记,以防误用。这些标记宜符合书面程序。程序宜包含对产品校准状况的识别。宜开出不符合项以记录所采取的措施。该程序宜包括发现设备出现校准故障时应采取的措施计划。

4) 检查

检查包括以下内容:

i) 设备

宜制定一份包含所有安全设备的清单(针对所有项目使用唯一标识)。宜按要求检查这些设备,以并纳入检查方案;

ii) 安全检查

宜进行安全检查,但不能免除经授权的人员进行日常检查或识别安全威胁的责任;

iii) 检查记录

宜保存每次安全检查的记录。记录宜表明是否按要求执行文件安全程序。宜对安全检查、巡视、调查和安全管理体系审核的记录进行抽样,以便识别潜在的不符合和反复出现的安全风险的根本原因。宜采取所有必要的预防措施。对于检查过程中发生的安全威胁情况和识别的不合格设备宜记录为不符合项,根据不符合程序评估风险并予以纠正。

5) 供应商(承包商)的设备

承包商使用的安全设备宜受到与组织内部的设备同样的控制。承包商要求提供保证确保其设备符合要求。工作开始前,对于识别出的所有关键设备,供应商宜提供所需的设备测试和维护记录复本。如果任何任务要求特殊培训,相应培训记录宜应提供给消费者以供查看。

6) 统计或其他理论分析技巧

用于评估安全形势、调查安全事件或故障,或帮助确定安全决策的任何统计或其他理论分析技巧宜以正确的科学原则为基础。最高管理者宜确保对这些技巧的需求予以识别。适当时,宜记录其使用指南及其适用情况。

e) 典型输出

典型输出包括下列项目:

- 监视安全安排有效性的程序;
- 检查时间表和核查表;
- 设备检查清单;
- 安全设备清单;
- 校准安排和记录;
- 维护活动和结果;
- 完整清单和检查报告(安全管理体系审核输出,见 4.5.4);
- 不符合项报告;
- 以上程序执行结果的证据。

4.5.2 体系评价

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

组织应通过定期审查、测试、事后报告、经验教训、性能评估和演练来评估安全管理计划、程序和能力。同时，如果上述因素发生任何重大变化，则必须立即在相关程序中予以说明。 组织应定期评估是否符合相关法律法规、行业最佳实践及自身策略和目标的要求。 组织应对定期评估结果做好记录。

b) 目的

组织宜制定有效程序评审和评价安全管理计划、程序以及组织满足方针、目标和指标的能力。组织还应定期评审与适用监管要求的一致性。

这些程序的主要目的是确保安全计划和程序随着变化的需求和需要保持更新。这些变化宜及时且充分考虑供应链规范、最佳实践和所获经验的所有变化。

c) 典型输入

典型输入宜包括：

- 事件报告；
- 事件计划和预备演习结果；
- 威胁识别、风险评估和风险控制报告；
- 安全管理体系审核报告，包括不符合项报告；
- 事件和/或危险报告；
- 管理评审报告和措施(见 4.6)；
- 目标实现进程；
- 变更的监管要求；
- 不断变化的相关方和利益相关方的期望；
- 组织工作范围、活动和客户群的变化。

d) 过程

组织的管理层宜在适当时间间隔内评审安全管理体系，建立并确保其持续的适用性和有效性。间隔时间宜尽可能短，以便在后续损失产生前识别出体系的失效。

有效体系及其实施的结果、目标和方针宜满足持续改进(ISO 28000 的主要原则之一)。4.5.2 要求的过程和程序应确保实现以上内容。

e) 典型输出

典型输出和结果包括：

- 改进的过程和性能；
- 不符合项报告数量减少；
- 合法性；
- 最新的威胁识别、风险评估报告和风险登记表；
- 改进的过程；
- 所采取的纠正和预防措施的有效性的评估证据。

4.5.3 安全相关故障、事件、不符合项及纠正和预防措施

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

组织应制定、实施并维护用于确定以下职责和权力的程序：

a) 评估和启动预防性措施，以确定潜在安全故障，从而防止发生；

b) 安全相关调查：

1) 故障(包括漏报和虚假警报)；

2) 事件和紧急情况；

3) 不符合项；

c) 采取措施减轻上述故障、事件或不符合项造成的后果；

d) 启动和完成纠正措施；

e) 确认所采取纠正措施的效果。

根据这些程序的规定，在实施之前应通过安全威胁和风险评估流程对提出的所有纠正和预防措施进行审查，除非立即实施可即时防止对生命或公共安全造成影响。

为了消除实际和潜在不符合项而采取的任何纠正或预防措施应与问题的严重性相适合，并与可能遭受的安全管理相关威胁和风险相称。组织应实施并记录纠正和预防措施所带来的书面程序变化，并在必要时进行必要培训。

b) 目的

组织宜制定有效程序报告和评价和/或调查紧急情况、安全事件和不符合项。程序的主要目的是通过识别和处理根本原因预防情况的再次发生。此外，程序宜能够检测、分析和消除不符合项产生的潜在原因，包括人为、体系、过程或设备故障和失误原因造成的后果。

c) 典型输入

典型输入包括下列项目：

- 程序(总体)；
- 应急预案；
- 安全威胁识别、风险评估和风险管理；
- 安全管理体系审核报告，包括不符合项报告；
- 安全事件和安全威胁报告；
- 安全设备维修与使用报告。

d) 过程

组织应制定文件化程序以确保调查安全事件和不符合项，并实施纠正和/或预防措施。宜监视纠正和预防措施的实施进展和评审措施的有效性。

下列要素宜包括于过程中：

1) 程序

程序宜考虑下列内容：

i) 概述

程序宜：

- 确定负责实施、报告、调查、后续跟进及监视纠正和预防措施的人员的责任和权限；
- 要求汇报所有不符合项、安全事件和安全威胁；
- 适用于所有人员(即员工、临时工、承包商、来访者和供应链相关的其他任何人员)；
- 考虑对利益相关方的影响；
- 确保员工不会因报告安全事件而会受到指责；
- 确定对安全管理体系中识别的不符合项采取的一系列措施。

ii) 紧急措施

首次识别不符合项、安全事件或威胁时，宜采取纠正安全事件的紧急措施。

程序宜：

- 确定通知过程；
- 适当时，纳入应急预案与程序的协作；
- 确定与潜在或实际威胁相关的调查工作规模（包括对严重安全事件调查的管理）。

iii) 记录

宜采用适当方法记录有关紧急调查和后续详查的事实的信息和结果。

组织宜确保在以下方面遵循程序要求：

- 记录不符合项、安全事件或安全威胁的详细资料；
- 确定记录储存地点和存储责任。

iv) 调查

程序宜确定如何处理调查过程。程序宜识别：

- 待调查事件的类型（如可能导致严重威胁的事件）；
- 调查目的；
- 调查人员、调查人员的权限及所需资质（适当时，包括各级管理人员）；
- 不符合项的根本原因；
- 证人访谈安排；
- 实际问题，如摄像头的可用性和证据的存储；
- 调查报告安排，包括向相应的利益相关方汇报。

调查人员宜在开始对事实进行初步分析的同时进一步收集信息。数据收集和分析宜持续进行，直至获得充分且详尽的解释。

v) 纠正措施

纠正措施是识别不符合项和安全事件的根本原因以防再次发生而采取的措施。制定和保持纠正措施程序的要素示例包括：

- 短期和长期纠正和预防措施的确定和实施（同样包括适当的信息来源的使用，如具备安全技能的员工提出的建议）；
- 就对安全威胁识别和风险评估结果造成的任何影响（即更新安全威胁识别、风险评估和风险管理报告的任何需求）的评价；
- 记录因纠正措施或安全威胁识别、风险评估和管理而产生的所有必要的程序变更；
- 应用风险管理或修改现有风险管理，以确保采取纠正措施并保持有效。

vi) 预防措施

预防措施是用于预防出现潜在安全不符合项而采取的措施。

制定和保持预防措施程序的要素示例包括：

- 使用适当的信息来源，如纠正措施结果、安全事件趋势、安全管理体系审核报告、最新的风险评估、安全相关的新信息、具备安全技能的员工和利益相关方的建议等；
- 采取和实施预防措施并应用控制措施以确保其有效；
- 记录由预防措施引起的任何程序变更，并提交审批。

vii) 后续跟踪

采取的纠正或预防措施宜有效可行。宜检查所采取的纠正/预防措施的有效性。未完成/超期的措施宜尽早向最高管理者报告。

2) 不符合项和安全事件分析

宜定期分类和分析不符合项和安全事件的原因，以进行根本原因分析。频次和严重性等级宜由其他供应链利益相关方决定。

分类和分析宜包括以下内容：

- 可报告的安全事件的频次或严重性等级；
- 位置、相关活动、组织、日期和时间(适当时)；
- 类型和程度或对设施和供应链的影响等；
- 直接原因和根本原因。

宜充分注意安全事件。所有安全事件均有可能是发生安全威胁或伤害的迹象。

宜得出有效结论并采取有效措施。该分析宜提交给最高管理者，并纳入管理评审(见 4.6)。

3) 监视和沟通结果

宜评估安全调查和报告的有效性。评估宜客观并提供定量结果(如可能)。

从调查中汲取经验的组织宜：

- 识别组织安全管理体系和综合管理中缺陷产生的根本原因(适用时)；
- 向管理层和相关利益相关方沟通结果和建议(见 4.4.3)；
- 将相关的调查发现和建议纳入持续的安全评审过程；
- 监视补救控制措施的及时实施情况及后续有效性；
- 在整个组织及其控制并影响的供应链范围内应用从不符合项和安全事件调查中汲取的经验，关注所涉及的概括性原则，而非局限于用来避免组织同一区域出现类似事件的具体措施。

4) 记录保持

记录保持可迅速完成，至少可为正式的策划，也可为复杂、长期的活动。相关文件宜适用于纠正措施的级别。

报告和建议宜提交给最高管理者的代表分析和保留(见 4.5.4)。

组织宜保存安全事件记录。供应链监管组织可能需要此类记录。

e) 典型输出

典型输出包括下列项目：

- 安全事件和不符合项程序；
- 不符合项报告；
- 不符合项记录；
- 调查报告；
- 最新安全风险识别、风险评估和风险管理报告；
- 管理评审输入；
- 所采取的纠正和预防措施的有效性评价证据。

4.5.4 记录的控制

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织在必要时应建立并保存记录，以证明符合其安全管理体系和本文件的要求并证明各项结果满足要求。
>
> 组织应制定、实施并维护记录识别、存储、保护、检索、保留和销毁相关程序。
>
> 各记录应清晰可辨，且具有可追踪性。
>
> 电子和数字文件宜防止篡改、进行安全备份，并且只能为被授权人员所用。

b) 目的

宜保存记录以证明安全管理体系有效运行。宜制定和保存支持管理体系和满足要求的安全记录，并宜清晰和充分识别。

c) 典型输入

保存的记录(用于证明满足要求)宜包括下列内容:

- 培训和能力记录;
- 安全检查报告;
- 安全不符合项;
- 预防和纠正措施结果;
- 安全管理体系审核报告;
- 安全会议纪要;
- 安全演习和演练报告;
- 管理评审;
- 安全威胁识别、风险评估和风险管理记录。

d) 过程

ISO 28000 中的要求在很大程度上是不言自明的。然而,宜另外考虑以下内容:

- 安全记录的处理权限;
- 安全记录的保密性(保护标志);
- 安全记录保留的相关法律及其他要求;
- 电子记录使用相关问题。

安全记录宜填写完整、清晰并可充分识别。宜规定安全记录的保留时间。记录宜存储在安全的地方,便于检索并防止损坏。根据具体情况和法律要求,关键安全记录宜防火或防止其他损坏。

e) 典型输出

典型输出包括下列项目:

- 程序(用于安全记录的识别、保存和处理);
- 保存完好和便于检索的安全记录。

4.5.5 审核

在 ISO 28000 中的要求、目的、典型输入、过程和典型输出包括以下方面。

a) ISO 28000 要求

> 组织应制定、实施并维护安全管理审计方案,并应确保按照所计划的间隔时间对安全管理体系进行审计,以便:
>
> a) 确定安全管理体系是否满足下列要求:
>
> 1) 是否符合安全管理的计划安排要求,包括本文件第 4 章全部要求;
>
> 2) 是否正确贯彻实施;
>
> 3) 在遵守组织安全管理策略和目标时是否有效;
>
> b) 审查以往的审计结果以及不符合项的纠正措施;
>
> c) 向管理层提供有关审计结果的信息;
>
> d) 验证相关安全设备和人员是否正确部署。
>
> 审计方案(包括任何计划表)应以组织活动的威胁和风险评价结果及以往的审计结果为基础。审计程序应包括范围、频率、方法和能力,以及审计和报告结果的责任和要求。在可能的情况下,应由与被审查活动直接责任人员无关的人员进行审计。
>
> 注:"与……无关的人员"未必是指组织的外部人员。

b) 目的

组织安全管理体系的内部审核宜在计划的时间间隔内实施,以便确定并向管理层告知该体系是否

满足程序要求和 ISO 28000:2007 中第 4 章的全部要求，以及是否正确贯彻实施这一体系。内部审核还可用于识别组织安全管理体系的改进时机。通常情况下，安全管理体系审核需要考虑适用于供应链的安全策略和程序以及条件和实践。

宜制定内部安全管理体系审核方案，以便组织评审其安全管理体系是否满足 ISO 28000 及其他运行范围内的要求。拟定的安全管理体系审核宜由组织内部和/或其指定的外部人员执行，以便确定与文件安全程序的符合度，并评价该体系是否有效满足组织安全目标。安全管理体系审核人员宜能够做到公正客观。

注：内部安全管理体系审核关注安全管理体系绩效。不得与安全、评审、评估或其他安全检查混淆。

c) 典型输入

典型输入包括下列项目：

- 安全策略声明；
- 安全目标；
- 安全程序和说明；
- 安全威胁识别、风险评估和风险管理结果；
- 法规和最佳实践(如适用)；
- 不符合项报告；
- 安全管理体系审核程序；
- 有能力的独立内部/外部审核员；
- 不符合项程序；
- 安全演习和演练；
- 来自外部组织的安全威胁信息。

d) 过程

1) 审核

安全管理体系审核就组织是否符合安全程序和实践提供了全面且正式的评估。

安全管理体系审核宜根据计划安排进行。必要时，可实施追加审核。如发生影响安全体系的事件，或组织、设施或供应链范围发生变更。

只有有能力的独立人员(接受关于审核区域的安全调查)才能执行安全管理体系审核。

安全管理体系审核的输出宜包括对安全程序有效性及程序和实践的符合程度的详细评估，且必要时，宜识别纠正措施。安全管理体系审核结果宜及时记录并向管理层报告。

注：GB/T 19011—2003 描述的一般原则和方法适用于安全管理体系审核。

2) 计划表

通常，宜制定年度计划以便安排内部安全管理体系审核进度。安全管理体系审核宜阐明安全管理体系涵盖的所有运行，并评价其是否满足 ISO 28000 的要求。

安全管理体系审核的频次和范围宜与风险相关，风险涉及安全管理体系各要素、安全管理体系绩效的可用数据和管理评审输出，同时宜与安全管理体系范围或受变化影响的运行环境相关。

另外，当出现必须执行审核的情况时，如安全事件发生后，虽未安排计划，也宜实施安全管理体系审核。

3) 管理者的支持

安全管理体系审核要发挥价值，最高管理者必需完全致力于践行审核这一概念，并在组织内部有效执行。最高管理者宜考虑审核结果和建议，必要时且在恰当时间采取适当措施。一旦同意进行安全管理体系审核，宜采取公正方法实施审核。宜告知所有相关人员审核目的和益处。宜激励工作人员与审核员给予充分配合审核员，并如实和建设性地回答他们提出的问题。

4) 审核员

安全管理体系审核可由一人或多人进行。通过组队可扩大参与度并促进合作，还可广泛利用专业人员的技能和知识。

审核员宜独立于组织的任何部分或有待审核的活动，必要时，宜接受审核区域的安全调查。

审核员需了解其任务并具备相应的执行能力。他们需要具备有关相关标准、实用规范和审核体系的经验和知识，以便评估绩效和识别缺陷。审核员宜熟悉所有相关法规规定的要求。此外，审核员还宜了解并可使用其工作相关的标准和权威指南。

5) 数据收集和解释

用于信息收集的技巧和辅助设备取决于所进行的安全管理体系审核的性质。安全管理体系审核宜确保对重要活动进行代表性抽样审核，并对相关人员(适当时，包括员工安全代表)进行访谈。宜评审相关文件，包括：

- 安全管理体系文件；
- 安全策略声明；
- 安全目标；
- 安全演习和演练的结果；
- 程序；
- 安全会议纪要；
- 安全执行组织或其他监管组织的所有报告或沟通信息(口头、信件、通知等)；
- 法定登记簿和证书；
- 培训记录；
- 以往的安全管理体系审核报告；
- 纠正措施要求；
- 不符合项报告。

可行时，宜检查安全管理体系审核程序，避免误解或误用收集的资料、信息或其他记录。

6) 审核结果

最终的安全管理体系审核报告内容宜清晰、准确和完整，由审核员注明日期并签字。根据具体情况，宜包括下列要素：

- 安全管理体系审核的目标和范围；
- 安全管理体系审核计划的详细资料、审核小组成员和受审核方代表的身份、审核日期及受审核区域的确定；
- 用于安全管理体系审核的参考文件(如 ISO 28000 和安全管理手册)的识别；
- 确定不符合项的详情；
- 审核员关于与 ISO 28000 符合度的评估；
- 安全管理体系实现所述安全管理目标的能力；
- 最终的安全管理体系审核报告的发布。

宜尽快将安全管理体系审核结果反馈至所有相关方，以便采取纠正措施。宜就商定的补救措施制定行动计划，同时确定负责人、完成日期和报告要求。宜确定后续监测安排以确保建议的有效执行。

管理层宜评审结果，且必要时，宜采取有效措施。

宜进行后续(不定期)审核以便评审纠正措施是否得以有效执行。

在记录安全管理体系审核报告内的信息时，宜考虑其保密性。

e) 典型输出

典型输出包括下列项目：

- 安全管理体系审核计划/方案；
- 安全管理体系审核程序；

- 安全管理体系审核报告，包括不符合项报告、建议和纠正措施要求；
- 经签署的/关闭的不符合项报告；
- 向管理层报告安全管理体系审核结果的证明。

4.6 管理评审和持续改进

管理评审和持续改进涉及以下方面，管理评审与其他要素的关系见图 6。

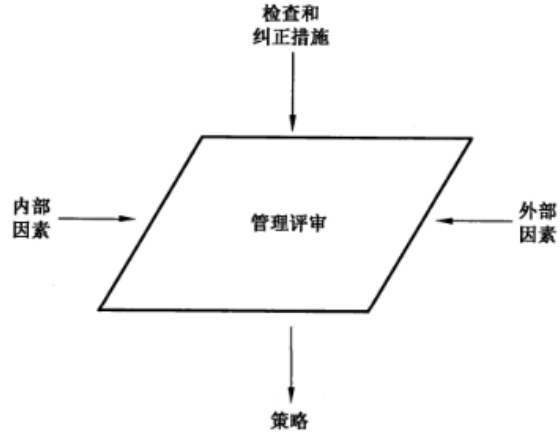

图 6 管理评审

a) ISO 28000 要求

最高管理者应按照所计划的时间间隔，对组织的安全管理体系进行审查，以确保其持续适用性、适当性和有效性。审查应包括评价安全管理体系的改善时机和变更需求(包括安全策略及安全目标、威胁和风险)。应保存管理审查记录。管理审查应包括以下内容：

a) 审计结果以及有关是否符合法律要求及组织认可的其他要求的评估情况；
b) 与外部相关方的沟通情况，包括投诉；
c) 组织的安全业绩；
d) 目标和指标范围；
e) 纠正和预防措施状况；
f) 根据先前管理审查情况所采取的后续措施；
g) 不断变化的情况，包括与其安全有关的法律和其他要求的发展变化情况；
h) 改善建议。

管理审查的成果应包括任何与安全管理体系的安全策略、目标、指标和其他要素潜在变化相关，且符合持续改进要求的决策和措施。

b) 目的

最高管理者宜评审安全管理体系的运行情况，以便评价其是否充分实施和保持实现组织安全策略和目标的适宜性和有效性。

评审宜考虑安全策略是否继续适合。为适合未来需求，宜确定新的或更新的安全目标以进行持续改进，并考虑是否需要变更安全管理体系的要素。

c) 典型输入

典型输入包括下列项目：

- 内部和外部安全管理体系审核的结果；
- 上次评审以来针对体系采取的纠正措施；

- 安全演习和演练报告；
- 最高管理者代表关于体系总体绩效的报告；
- 组织人员和利益相关方关于体系有效性的报告(如对供应链产生影响)；
- 安全威胁识别、风险评估和风险管理过程的报告；
- 培训和意识培养计划的有效性；
- 安全管理目标的进展和有效性。

d) 过程

管理评审过程一般包括最高管理者定期召开的会议(如年度会议)。评审宜关注安全管理体系的总体绩效而非具体细节，因为具体细节可通过安全管理体系内部的常规方法处理。

在策划管理评审时，宜考虑以下内容：

- 所阐述的主题；
- 参加人员(管理人员、安全专家顾问及其他人员)；
- 评审相关的参与者的职责；
- 有待评审的信息。

评审宜阐述下列主题：

- 当前安全策略的适用性；
- 制定和更新安全目标以便今后进行持续改进；
- 当前安全威胁识别、风险评估和风险管理过程的充分性；
- 当前风险水平和现有控制措施有效性；
- 资源的充足性；
- 安全检查过程的有效性；
- 安全风险报告过程的有效性；
- 安全数据和已发生的事件；
- 无效程序记录情况；
- 自上次评审以来实施的内部和外部安全管理体系审核的结果及其有效性；
- 紧急情况准备状态和安全恢复安排；
- 安全管理体的改进；
- 安全事件调查的输出；
- 对法律、法规、技术或安全情报和信息的可预见变更影响的评价。

最高管理者宜确保在管理评审会议中报告安全管理体系的总体绩效。必要时，可在一定时间间隔内对安全管理体系绩效采取部分评审。必要时，增加频次。

管理评审可包括整合管理体系评审，因此同一会议或相同过程中可以考虑安全、质量及其他管理体系要素的输出。如果采用该方法，不宜淡化组织整合管理体系任一组成部分的重要性。

e) 典型输出

典型输出包括下列项目：

- 所有评审会议的纪要；
- 安全策略和安全目标的修改；
- 个别管理人员采取的具体纠正措施及完成的预期日期；
- 具体改进措施，以及分配职责和预期完成的日期；
- 纠正措施评审的日期；
- 未来内部安全管理体系审核策划中体现重点区域。

附 录 A
（资料性）
ISO 28000:2007 与 GB/T 24001—2004 和 GB/T 19001—2000 之间的对应关系

ISO 28000:2007 与 GB/T 24001—2004 和 GB/T 19001—2000 之间的对应关系见表 A.1。

表 A.1 ISO 28000:2007 与 GB/T 24001—2004 和 GB/T 19001—2000 之间的对应关系表

ISO 28000:2007		GB/T 24001—2004		GB/T 19001—2000	
供应链安全管理体系要求（仅标题）	4	环境管理体系要求（仅标题）	4	质量管理体系要求（仅标题）	4
一般要求	4.1	一般要求	4.1	一般要求	4.1
安全管理方针	4.2	环境方针	4.2	管理承诺 质量方针 持续改进	5.1 5.3 8.5.1
安全风险评估和策划（仅标题）	4.3	策划（仅标题）	4.3	策划（仅标题）	5.4
安全风险评估	4.3.1	环境因素	4.3.1	客户关注焦点 确定产品相关要求 评审产品相关要求	5.2 7.2.1 7.2.2
法律、法规及其他安全监管要求	4.3.2	法律及其他要求	4.3.2	客户导向 确定产品相关要求	5.2 7.2.1
安全管理目标	4.3.3	目标、指标和方案	4.3.3	质量目标 质量管理体系策划 持续改进	5.4.1 5.4.2 8.5.1
安全管理指标	4.3.4	目标、指标和方案	4.3.3	质量目标 质量管理体系策划 持续改进	5.4.1 5.4.2 8.5.1
安全管理方案	4.3.5	目标、指标和方案	4.3.3	质量目标 质量管理体系策划 持续改进	5.4.1 5.4.2 8.5.1
实施与运行（仅标题）	4.4	实施与运行（仅标题）	4.4	产品实现（仅标题）	7
安全管理结构、权限和职责	4.4.1	资源、角色、职责和权限	4.4.1	管理承诺 职责和权限 管理代表 资源供应 基础设施	5.1 5.5.1 5.5.2 6.1 6.3
能力、培训和意识	4.4.2	能力、培训和意识	4.4.2	（人力资源）概述 能力、意识和培训	6.2.1 6.2.2

表 A.1 ISO 28000:2007 与 GB/T 24001—2004 和 GB/T 19001—2000 之间的对应关系表（续）

ISO 28000:2007		GB/T 24001—2004		GB/T 19001—2000	
沟通	4.4.3	沟通	4.4.3	内部沟通	5.5.3
				顾客沟通	7.2.3
文件	4.4.4	文件	4.4.4	(文件要求)概述	4.2.1
文件和资料管理	4.4.5	文件管理	4.4.5	文件管理	4.2.3
运行控制	4.4.6	运行控制	4.4.6	产品实现策划	7.1
				确定产品相关要求	7.2.1
				评审产品相关要求	7.2.2
				设计开发策划	7.3.1
				设计开发投入	7.3.2
				设计开发输出	7.3.3
				设计开发评审	7.3.4
				设计开发验证	7.3.5
				设计开发确认	7.3.6
				设计开发变更控制	7.3.7
				采购流程	7.4.1
				采购信息	7.4.2
				采购产品验证	7.4.3
				产品和服务供应管理	7.5.1
				产品和服务供应流程确认	7.5.2
				产品保存	7.5.5
应急准备、响应和安全恢复	4.4.7	应急准备和响应	4.4.7	不合格产品管理	8.3
检查和纠正措施(仅标题)	4.5	检查(仅标题)	4.5	测量、分析与改进(仅标题)	8
安全绩效测量和监视	4.5.1	监视和测量	4.5.1	监视和测量设备的控制	7.6
				概述(测量、分析与改进)	8.1
				监测流程	8.2.3
				产品监测	8.2.4
				数据分析	8.4
体系评价	4.5.2	合规性评价	4.5.2	过程监测	8.2.3
				产品监测	8.2.4
安全相关缺陷、事件、不符合项及纠正和预防措施	4.5.3	不合格项及纠正和预防措施	4.5.3	不合格产品控制	8.3
				数据分析	8.4
				纠正措施	8.5.2
				预防措施	8.5.3

表 A.1 ISO 28000:2007 与 GB/T 24001—2004 和 GB/T 19001—2000 之间的对应关系表（续）

ISO 28000:2007		GB/T 24001—2004		GB/T 19001—2000	
记录管理	4.5.4	记录管理	4.5.4	记录管理	4.2.4
审核	4.5.5	内审	4.5.5	内审	8.2.2
管理评审和持续改进	4.6	管理评审	4.6	管理层承诺	5.1
				管理评审(仅标题)	5.6
				总则	5.6.1
				评审输入	5.6.2
				评审输出	5.6.3
				持续改进	8.5.1

参 考 文 献

[1] GB/T 19001—2000 质量管理体系 要求
[2] GB/T 19011—2003 质量和(或)环境管理体系审核指南
[3] GB/T 24001—2004 环境管理体系 要求及使用指南
[4] GB/T 27021—2007 合格评定 管理体系审核认证机构的要求
[5] ISO 28000:2007 Specification for security management systems for the supply chain
[6] 全球贸易安全与便利标准框架
[7] 海关-贸易伙伴关系(C-TPAT)指南
[8] 欧盟授权经济经营者(AEO)条例