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。

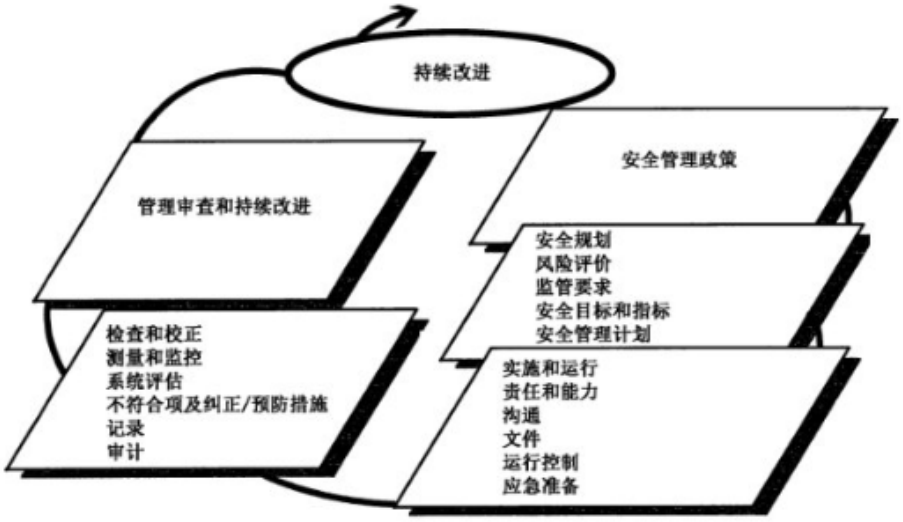

图1　成功安全管理的要素

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。

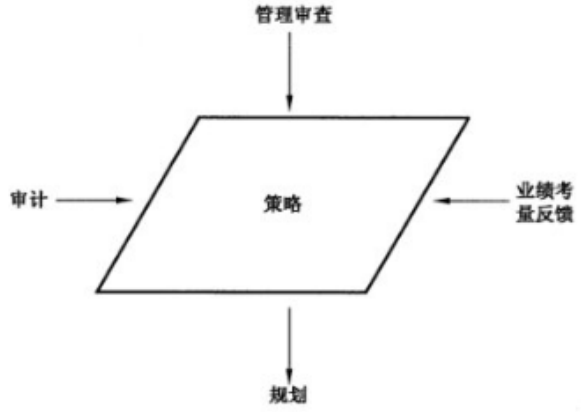

图 2 安全管理策略

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。

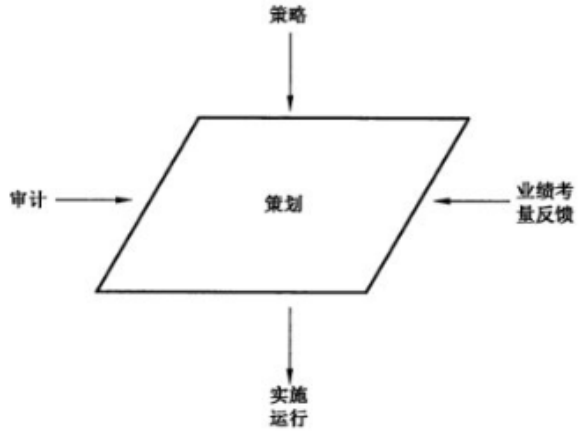

图 3 策划

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

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。

- 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。

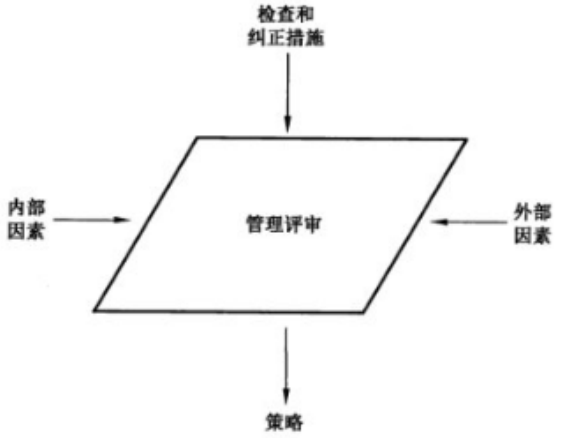

图 6 管理评审

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