供应链安全管理体系认证依据

目录

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。

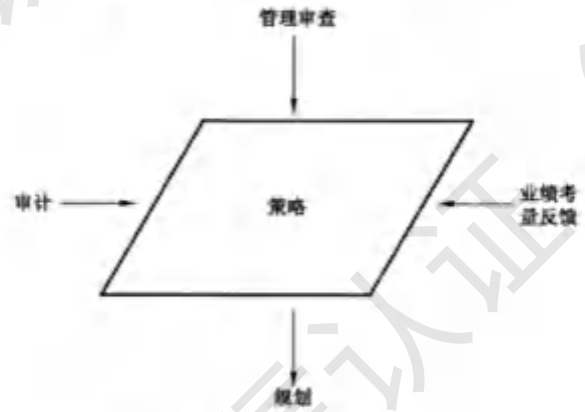

图 2 安全管理策略

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。

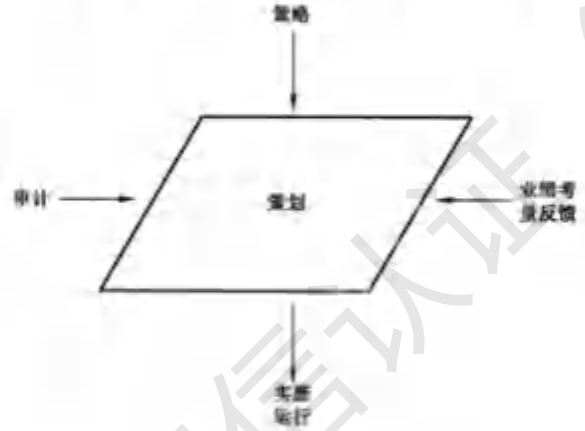

图3 策划

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。

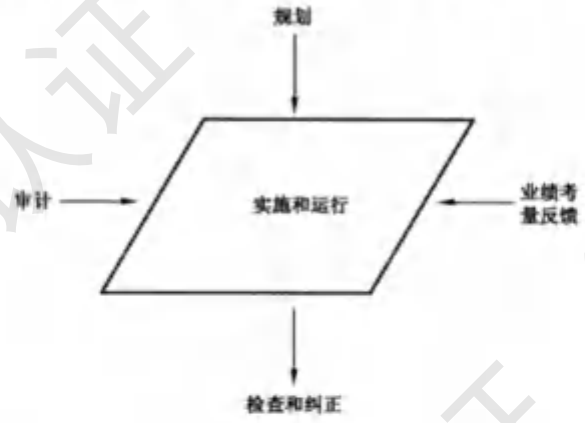

图 4 实施和运行

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。

c） 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。

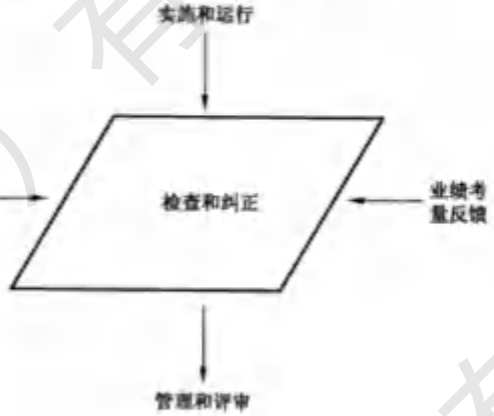

图 5 检查和纠正措施

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。

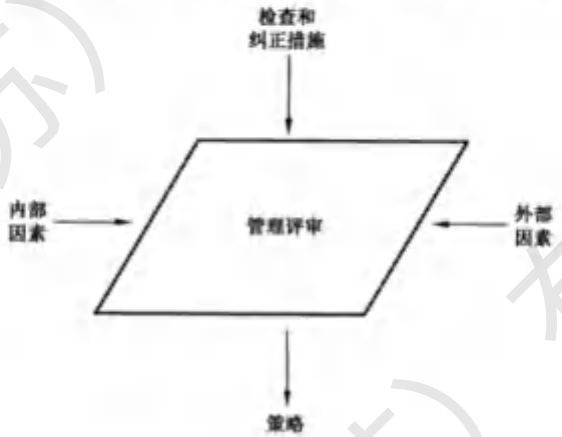

图 6 管理评审

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

ICS 03.100.01
CCS A 10

中华人民共和国国家标准

GB/T 43632—2024/ISO 28002:2011

供应链安全管理体系　供应链韧性的开发要求及使用指南

Security management systems for the supply chain—Development of resilience in the supply chain—Requirements with guidance for use

（ISO 28002:2011，IDT）

2024-03-15 发布　　2024-07-01 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。

本文件等同采用ISO 28002:2011《供应链安全管理体系 供应链韧性的开发 要求及使用指南》。

本文件做了下列最小限度的编辑性改动:

a) 增加了第4章出现的图4的引出语;

b) 删除了4.3中与正文无关的"(见4.4)";

c) 调换了资料性附录C和资料性附录D的顺序。

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、江苏省质量和标准化研究院、云南建投物流有限公司、诺力智能装备股份有限公司、中信戴卡股份有限公司、美的集团股份有限公司、新疆维吾尔自治区标准化研究院、浪潮工创(山东)供应链科技有限公司、贵州习酒投资控股集团有限责任公司、中国港湾工程有限责任公司、漳州片仔癀药业股份有限公司、南京医药股份有限公司、中武(福建)跨境电子商务有限责任公司、南方电网大数据服务有限公司、河北邯郸丛台酒业股份有限公司、诚天国际供应链(深圳)有限公司。

本文件主要起草人:秦挺鑫、管旭琳、刘珏、李军、孔肖蓥、王皖、许歆宜、蒋兴祥、钟锁铭、孟祥程、陈林、王少华、傅炜、郭鑫、杜德喜、黄金、陈强、周倩、何灿、白银战、何俊彪、洪绯、马云涛、张金花、郭珅、赵永国、李鹏亮、冯凌炬。

引言

0.1 概述

全球各地组织正在加快制定风险管理和韧性方案，以解决各自目标实现过程中的不确定性。由于组织需保证自己的供应商及扩展供应链已经规划并采取措施以预防和减轻其所面临的威胁和危险，故而迫切需要相关标准和最佳实践。为确保供应链的韧性，组织必须开展全面系统的预防、保护、准备、减缓、响应、连续性和恢复等一系列工作。

供应链中组织的生存性在很大程度上取决于其供应商和客户的韧性。因此，在供应链中融入韧性以及提高供应链中组织的韧性必须集中在组织内部及其外部供应商和客户。

供应链中断期间，必须强调：对于中断的确切性质，一开始可能无法完全理解，只能随着时间的推移才能充分理解。因此，制定的韧性计划和方针宜强调对新信息的适应和持续评估，以确保所采取措施的适当性。供应链中断程度严重时，很有可能引起新闻媒体的关注。若未能妥善管理与新闻媒体的关系，则可能会对恢复响应活动产生负面影响，进而使利益相关方失去信心。这种信心丧失可能导致客户流失、政府或金融组织对信息的需求增加，以及外部组织设定限制条件。本文件适用于私营、非营利、非政府和公共部门环境，它是行动计划和决策的管理框架，可用于预测和预防（如可行）中断性事件（紧急情况、危机、灾害）及针对该类事件做好准备和应对。在管理体系中执行本文件，能够提高组织在相关事件中的管理和生存能力，并能通过采取一切适当措施帮助确保组织的持续生存能力。无论哪类组织，其领导层都有责任制定生存计划，确保利益相关方的权益。本文件正文部分提供了可审核性标准，用于建立、检查、保持和改进管理体系中执行的韧性方针，以加强针对中断性事件的预防、准备（预备）、减缓、响应、连续性和恢复工作。

本文件旨在成为供应链安全管理体系的组成部分。此外，对于遵循“策划 实施 检查 处置”（Plan-Do-Check-Act；PDCA）模式的组织，其内部其他管理体系中也可融入本文件。如果选择第三方独立认证，则将对包含本文件在内的整体管理体系标准进行认证。

通过采用具有适应性、主动性和被动性的综合恢复方法，可以利用组织内各部门和个人的观点、知识和能力。由于组织面临的许多自然、有意或无意的威胁和危险的概率相对较低，但造成的后果可能十分严重，综合方法允许组织在经济合理的情况下确定处理自身风险管理需求时的优先顺序。

0.2 供应链环境

对供应链中的风险进行管理时，需要了解组织环境以及整个供应链的全球环境背景。组织供应链中的各个节点涉及了计划、原料、制造、交付和退货等一系列风险和管理过程。所有这些管理过程都宜包含在组织的整体韧性方针中。在此条件下，组织将确定其供应链中包含韧性方案的级别和层级。

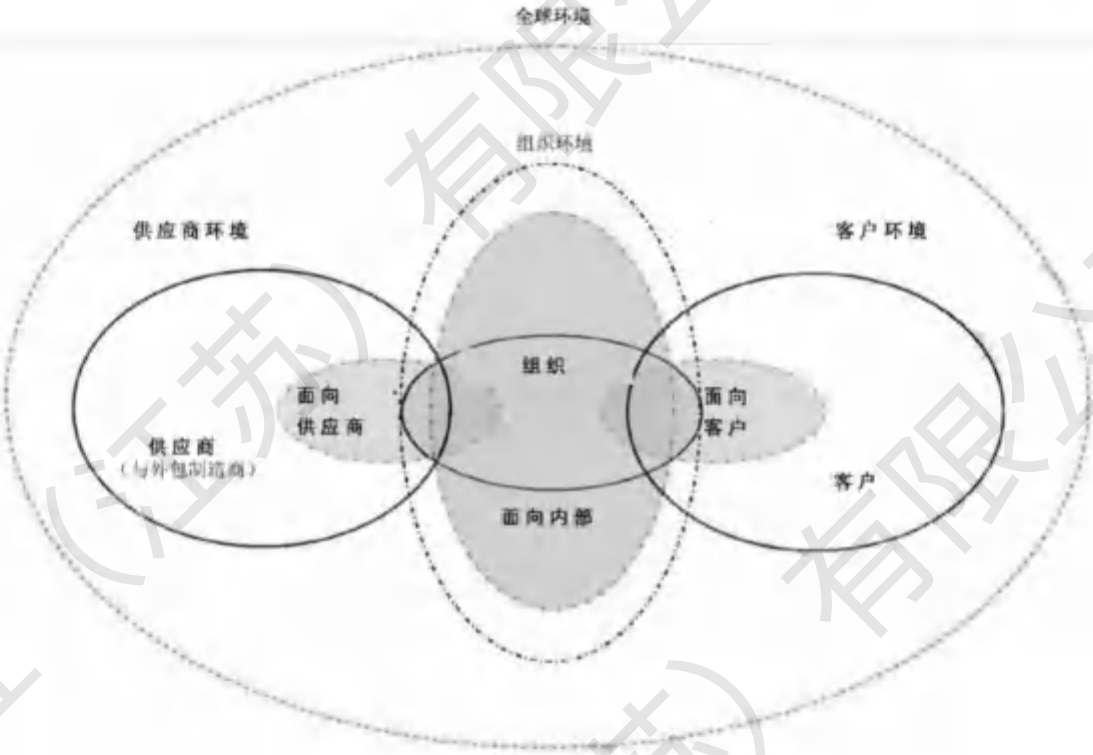

图 1　供应链中的韧性管理方针[资料来源：国际供应链协会(SCC)2007 年]

0.3　过程方法

管理体系方法鼓励组织进行组织需求和利益相关方需求分析并确定有助于成功的各类过程。管理体系提供了持续改进框架，以提高在加强安全性、准备、响应性、连续性和韧性方面的可能性。同时，管理体系还为组织及其客户提供了信心，即组织能够提供满足组织和利益相关方要求的安全、可靠的环境。

本文件采用过程方法，用于建立、执行、运行、监视、评审、保持和改进组织对供应链中断的韧性。组织需要对许多活动加以确认和管理，以确保有效运作。任何包含资源利用并进行管理，并将输入转化为输出的活动都可视为一个过程。通常，一个过程的输出会直接成为下一过程的输入。

组织内一套过程的应用，以及这些过程的识别和相互作用及其管理可以称为“过程方法”。

图 2 描述了本文件中提出的供应链韧性管理过程方法，鼓励使用者强调下列各方面的重要性：

a)　了解组织的风险、安全性、准备、响应、连续性和恢复要求；

b)　制定风险管理方针和目标；

c)　执行控制措施，以便在组织目标背景下对组织风险进行管理；

d)　监视并评审韧性管理方针的绩效和有效性；

e)　根据目标测评持续改进。

图 2　供应链韧性管理过程方法

0.3.1　制定供应链韧性方案并应用资源：

——将供应链风险管理视为重中之重；

——确保最高管理者支持供应链韧性方案；

——确保方案执行所需的资源到位。

0.3.2　确立供应链和韧性目标：

——确立供应链范围并映射到供应链；

——确立主题供应链中的风险管理目标。

0.3.3　识别供应链风险：

——全面评审供应链以识别风险；

——尽可能记录已识别的风险。

0.3.4　风险量化和区分优先级：

——根据发生的可能性和潜在影响量化每个风险；

——根据确定的目标使用风险量化来区分风险优先级。

0.3.5　执行风险应对方案：

——根据每个风险的优先级制定风险管理措施；

——根据降低风险发生的可能性和影响来定义每项措施的价值；

——针对确定的措施制定并执行计划。

0.3.6　监视供应链环境，以识别风险：

——持续监视供应链环境，以识别风险事件或前兆；

——当阈值被触发时，执行适用的减缓措施；

——记录采取措施后的评审和方案结果。

0.4　“策划—实施—检查—处置”（PDCA）模式

本文件旨在纳入使用“策划—实施—检查—处置”（PDCA）模式的管理体系，该模式反过来又将指导韧性管理方针流程的实施和整合。图 3 说明了管理体系中如何纳入韧性管理方针；该方针能够接收相关方的要求和期望，并通过必要的行动和流程产生符合这些要求和期望的风险管理结果。图 3 还说

明了本文件第4章中介绍的各流程间的关联。

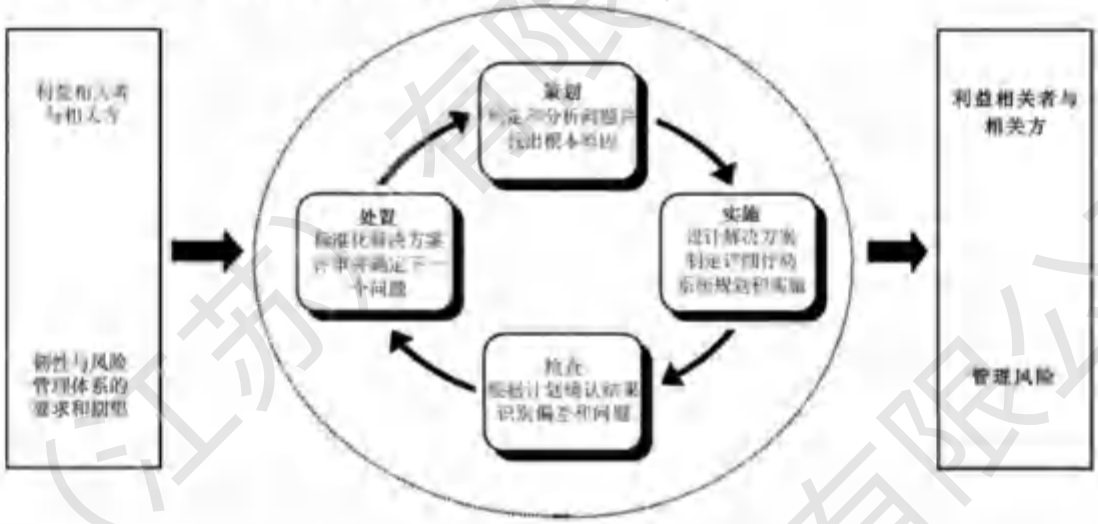

图3 包含韧性方针的管理体系流程图

策划 （建立管理体系）	建立与管理风险和提高安全性、准备、减缓、响应、连续性和恢复相关的管理体系方针、目标、流程和程序，以便按照组织的总体方针和目标交付结果
实施 （执行和运行管理体系）	执行和运行管理体系方针、控制措施、过程和程序
检查 （监视和评审管理体系）	根据管理体系方针、目标和实践经验对过程性能进行测评，并将结果上报管理者评审
处置 （保持和改进行管理体系）	根据内部管理体系审核和管理评审结果，采取纠正和预防措施，持续改进管理体系

对于将本文件作为一项方针纳入其中的管理体系，可通过与ISO 28000:2007、ISO 14001:2004和/或ISO/IEC 27001:2005的方法及PDCA模式相兼容且相符合的审核过程验证其合规性。

有关本文件使用的参考指南见附录B。有关本文件的使用限制的更多信息见附录C。本文件所使用的术语惯例见附录D。

本文件提供了通用要求作为框架，适用于组织（或组织部门），而与组织规模及其在供应链中的功能无关。本文件为组织在制定自身具体绩效标准时提供指导，使得组织能够制定和执行适合本组织及其利益相关方需求的韧性管理方针。

本文件强调组织在复杂多变环境中的韧性和适应能力，以及对关键供应链资产和过程的保护。应用本文件，组织能更容易地预防各种有意、无意和/或自然造成的中断性事件并做好相应准备（如有可能）和应对，而这类事件如不加以管理，可能会升级为紧急状况、危机或灾害。本文件涵盖了中断性事件发生前、发生期间和发生后的事件管理的所有阶段。

本文件为组织提供了一个框架，用于：

a) 制定一套预防、保护、准备、减缓和响应/连续性/韧性方针；

b) 建立实现方针承诺的目标、程序和过程；

c) 确保具备相关能力、意识和培训；
d) 设置衡量绩效及证明成功的标准；
e) 根据需要采取行动措施，以提高绩效；
f) 本文件是证明管理体系合格的必要条件；
g) 建立持续改进过程并予以应用。

附录A提供了关于体系策划、执行、测试、保持和改进的参考指南。

供应链安全管理体系 供应链韧性的开发要求及使用指南

1 范围

本文件规定了供应链韧性管理方针的要求，以便相关组织制定并执行相关方针、目标和方案，同时考虑到：

a) 组织需遵守的法律法规及其他要求；

b) 关于可能对组织及其利益相关方和供应链造成影响的重大风险、危害和威胁的信息；

c) 对组织资产和流程的保护；

d) 中断性事件管理。

本文件适用于被组织识别为可控制、改变或降低的风险以及无法预测的风险。本文件本身并未说明具体的绩效标准。本文件中的所有要求旨在应用于各组织各类基于 PCDA 模式的管理体系中。本文件提供了前述应用所需的各类要素(包括与技术、设施、流程和人员有关的要素)。本文件的适用范围取决于组织的风险接受能力和方针、组织的活动、产品和服务的性质和规模以及组织的运作地点和条件等因素。

本文件适用于具有以下需求的所有组织：

a) 针对本组织及其供应链建立一套韧性管理方针并予以执行、保持和改进；

b) 确保本组织符合其制定的韧性管理方针；

c) 通过下列方式展示本组织管理体系包含完善的韧性管理方针：

1) 自我决定和自我声明；

2) 寻求本组织相关各方(例如客户)对本组织是否合格进行确认；

3) 寻求组织外的一方对本组织自我声明进行确认；

4) 寻求外部组织对本组织的管理体系进行认证/注册。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO 28000:2007 供应链安全管理体系规范(Specification for security management systems for the supply chain)

3 术语和定义

下列术语和定义适用于本文件。

3.1

备用工作场所 alternate worksite

除主要工作场所以外的其他工作地点，以便在主要工作场所不可用时使用。

3.2

资产 asset

对组织有价值的任何东西。

注：资产包括但不限于人力资源、物质资源、信息资源、无形资源和环境资源。

3.3

审核 audit

为获得客观证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的，并形成文件的过程。

注1：内部审核，有时称为第一方审核，由组织自己或以组织的名义进行，用于管理评审和其他内部目的，可作为组织自我合格声明的基础。内部审核可以由与正在被审核的活动无责任关系的人员进行，以证实独立性。

注2：外部审核包括第二方和第三方审核。第二方审核由组织的相关方，如顾客或由其他人员以相关方的名义进行。第三方审核由外部独立的审核组织进行，例如提供对ISO 28000(即供应链安全管理体系标准)合格认证/注册的组织。

注3：当同时对两个或多个管理体系进行审核时，称为"组合审核"。

注4：当由两家或两家以上的审核组织合作对某一被审单位进行审核时，称为"联合审核"。

3.4

审核员 auditor

具有进行审核工作资格和能力的人员。

3.5

持续改进 continual improvement

为提高满足要求的能力而进行的重复性活动。

注：设定目标和发现改进时机的过程是一个通过使用审核结果和审核结论以及进行数据分析、管理评审或其他方式的持续过程，并且通常会需要采取纠正或预防措施。

3.6

合格 conformity

满足要求。

3.7

后果 consequence

某事件对目标影响的结果。

注1：一个事件可以导致一系列后果。

注2：后果可以是确定的，也可以是不确定的，对目标的影响可以是正面的，也可以是负面的。

注3：后果可以定性或定量表述。

注4：通过连锁反应，最初的后果可能升级。

[来源：GB/T 23694—2013，4.6.1.3]

3.8

连续性 continuity

由组织管理者事先批准的组织应对各类条件、情况和事件的战略和战术能力，以便在可接受的预定水平下继续组织运营。

注：本文件中所述连续性是对运营连续性和业务连续性的统称，以确保组织能够在正常运营条件之外继续运营。该条术语不仅适用于盈利性公司，也适用于所有性质的组织，如非政府组织、公益组织和政府组织。

3.9

纠正措施 corrective action

消除不合格的原因。

注 1：一个不合格可能有若干个原因。

注 2：采取纠正措施是为了防止再发生，而采取预防措施是为了防止发生。

3.10

危机 crisis

涉及即将发生的突然变化或重大变化、需要紧急关注并采取措施来保护生命、资产、财产或环境的不稳定情况。

3.11

危机管理 crisis management

整体管理流程，包括识别对组织产生威胁的潜在影响、提供实现韧性的框架以及有效应对的能力，以保护组织关键利益相关方的利益以及声誉、品牌、价值创造活动，同时有效恢复运营能力。

注：危机管理还包括发生事件时的准备、减缓响应、连续性或恢复管理以及通过培训、排练和评审确保准备、响应和连续性计划保持现行最新状态的总体方案的管理。

3.12

危机管理团队 crisis management team

负责指导响应计划和运营连续性计划的制定和执行，宣布运营中断或紧急/危机情况，并在恢复过程(包括中断前事件和中断后事件)中提供指导的一组人员。

注：危机管理团队可能包括组织内部人员以及直接和第一响应人、利益相关方和其他相关方。

3.13

关键性 critically

对目标、结果而言至关重要。

3.14

关键性分析 criticality analysis

根据组织使命和职能的重要性、处于危险中的人群或组织连续性中断事件的重要性对组织资产进行系统识别和评价的过程。

3.15

灾害 disaster

导致重大损害或损失的事件。

3.16

中断 disruption

导致正常运行、运营或流程中断的预见或未预见事件(如恶劣天气、社会安全事件、公用设施断电、技术故障或地震)。

注：中断原因包括会导致正常运行、运营或流程中断的正面或负面因素。

3.17

文件 document

信息和承载媒介。

注：上述承载媒介包括纸张、磁盘、电子或光学计算机光盘、照片或标准样本，或前述各类介质的组合。

3.18

紧急情况 emergency

紧急情况响应要求需要立即采取行动的突发、紧急事件，且通常为意外事件。

注：紧急情况通常是能预料或予以准备的中断事件或情况，但很少能准确预见。

3.19

演练 exercises

定期活动，旨在评估团队成员和工作人员在执行韧性管理方针方面的表现。

注 1：演练活动的目的是对团队成员和人员进行培训和训练，使其具备适当应对能力，以实现最佳表现。

注 2：演练可能包括激活预防、响应和/或连续性程序，但更可能涉及对已公布或未公布事件的模拟，其中参与者负责评估在事件实际发生之前可能出现哪些问题。

3.20

疏散 evacuation

在监督情况下将人员有组织、分阶段地从危险区域或潜在危险区域撤离至安全地点。

3.21

事件 event

某一类情形的发生或变化。

注 1：事件可以是一个或多个情形，并且可以由多个原因导致。

注 2：事件可以包括没有发生的情形。

注 3：事件有时也可以称为“事故”或“意外事件”。

注 4：没有造成后果的事件还可以被称为“未遂事件”“事件征候”“临近伤害”或“幸免”。

[来源：GB/T 23694—2013，4.5.1.3]

3.22

设施 facility

厂房、机械、物业、建筑、运输车辆、海港/陆路口岸/航空港及其他具有可量化业务功能和服务的基础设施项目或工厂和相关系统。

3.23

危险 hazard

潜在伤害的来源。

注：危险可能是一类风险源。

[来源：GB/T 23694—2013，4.5.1.4]

3.24

影响 impact

特定结果的评估后果。

3.25

影响(后果)分析 impact(consequence)analysis

对所有运营职能及运营中断可能对各职能产生的影响进行分析的过程。

注：影响分析是风险评价过程的一部分，包括业务影响分析；识别关键业务资产、职能、流程和资源以及评价组织因中断(或业务或运营环境改变)而可能遭受的潜在损害或损失(或业务或运营环境的变化)。通过影响分析，确定损失或损害的表现方式；事件发生后损害或损失可能随时间而升级的程度；使业务流程在最低可接受水平下继续运营所需最少服务和资源(人力资源、物质资源和财务资源)；组织活动、职能和服务宜得以恢复的时限和范围。

3.26

事故 incident

能够导致人身伤害、无形或物质资源损失，或导致组织运营、服务或职能中断的事件，而这类事件如不加以管理，可能会升级为紧急状况、危机或灾害。

3.27

完整性 integrity

保障资产准确性和完整性的性能。

3.28

可能性 likelihood

某件事发生的机会。

注：无论是以客观的或主观的、定性或定量的方式来定义、度量或确定，还是用一般词汇或数学术语来描述（如概率，或一定时间内的频率），在风险管理术语中，"可能性"一词都用来表示某事发生的机会。

[来源：GB/T 23694—2013，4.6.1.1]

3.29

管理计划 management plan

明确规定并形成文件的行动计划，通常包括执行管理过程所需的关键人员、资源、服务和行动。

3.30

减缓 mitigation

限制特定事件的各种负面后果。

3.31

互助协议 mutual aid agreement

两个或两个以上实体之间预先达成的、确保协议各方互相协助的协议。

3.32

不合格 nonconformity

不满足某项要求。

3.33

目的 objective

与组织自身设定需要达到的方针相一致的总体目标。

3.34

组织 organization

分配有责任、权力和关系的人员和设施的群体。

示例：公共或私人公司、法人团体、公司、企业、组织、慈善团体、独资经营商、协会，或上述单位的部分组合或全部组合。

3.35

方针 policy

由最高管理者正式表达的组织的总体意图和方向。

注：本文件中描述对其中一项此类方针（供应链韧性方针）的要求。

3.36

准备 preparedness

预备 readiness

在事件发生之前制定并执行的活动、计划和系统，可用于支持和加强对中断、紧急情况或灾害的预防、防护、减缓、响应和恢复。

3.37

预防 prevention

使组织能够避免、预防或限制中断发生的可能性或中断后果的措施。

3.38

预防措施 preventive action

消除潜在不合格或其他潜在不良因素的行为。

注 1：对于一项潜在不合格，可能由一种以上原因导致。

注 2：采取预防措施的目的在于预防发生，而采取纠正措施是为了防止复发。

3.39

危险和威胁预防　prevention of hazards and threats

用于避免、减少或控制任何类型的危险和威胁及其相关风险的过程、实践、技术、材料、产品、服务或资源，以减少其潜在可能性或后果。

3.40

概率　probability

对事件发生机会的度量，用 0 到 1 之间的数字表示。0 表示不可能发生，1 表示确定发生。

注：另见术语 3.28“可能性”。

[来源：GB/T 23694—2013，定义 4.6.1.4]

3.41

程序　procedure

为进行某项活动或过程所规定的途径。

注 1：程序能形成文件，也能不形成文件。

注 2：当有程序文件时，通常使用术语“书面程序”或“文件化程序”。包含程序的文件能称为“程序文件”。

3.42

记录　record

阐明所取得的结果或提供所完成活动的证据的文件。

注 1：记录能用于正式的可追溯性活动，并为验证、预防措施、和纠正措施提供证据。

注 2：通常，记录不需要控制版本。

3.43

剩余风险　residual risk

风险应对之后仍然存在的风险。

注 1：剩余风险中可能会包含未确认的风险。

注 2：剩余风险还能被称为“保留风险”。

[来源：GB/T 23694—2013，4.8.1.6]

3.44

韧性　resilience

组织对复杂多变环境的适应能力。

注 1：韧性是指组织能预防或阻止自身受到事件影响的能力，或在受到事件影响后能在可接受的时间内恢复到可接受水平的能力。

注 2：韧性是系统在面对内部和外部变化时保持其功能和结构的能力，并在必要时适度降低水平。

[来源：GB/T 23694—2013，4.8.1.7，有修改]

3.45

资源　resources

任何具有潜在价值并能使用的资产（人力资源、物质资源、信息资源或无形资源）、设施、设备、材料、产品或废弃物。

3.46

响应计划　response plan

以备应对事件而制定、编写和保存的程序和信息的各类书面文件。

3.47

响应方案　response program

有关维持和保护生命、财产、运营和关键资产所必需的活动和服务的开展计划、过程和资源。

注：响应步骤通常包括事件识别、通知、评价、声明、计划执行、通信和资源管理。

3.48

响应小组　response team

负责制定、执行、演练和保持包括过程和程序在内的响应计划的小组。

3.49

风险　risk

不确定性对目标的影响。

注 1：影响是指偏离预期，可以是正面的和/或负面的。

注 2：目标可以是不同方面（如财务、健康与安全、环境等）和层面（如战略、组织、项目、产品和过程等）的目标。

注 3：通常用潜在事件、后果或者两者的组合来区分风险。

注 4：通常用事件后果（包括情形的变化）和事件发生可能性的组合来表示风险。

注 5：不确定性是指对事件及其后果或可能性的信息缺失或了解片面的状态。

[来源：GB/T 23694—2013，2.1]

3.50

风险接受　risk acceptance

接受某一特定风险的决定。

注 1：风险接受可以不经风险应对，还可以在风险应对过程中发生。

注 2：接受的风险要受到监督和评审。

[来源：GB/T 23694—2013，4.7.1.6]

3.51

风险分析　risk analysis

理解风险的性质、确定风险等级的过程。

注 1：风险分析是风险评价和风险应对决策的基础。

注 2：风险分析包括风险估计。

[来源：GB/T 23694—2013，4.6.1]

3.52

风险评估　risk assessment

包括风险识别、风险分析和风险评价的全过程。

注：风险评价包括：确定内部和外部威胁和脆弱性、确定由此类威胁或脆弱性引发事件的可能性和影响、组织运营所必需的关键职能、明确减少风险所必需的控制措施以及评估这些控制措施的成本。

[来源：GB/T 23694—2013，4.4.1]

3.53

风险交流　risk communication

决策者与其他利益相关方之间交流或分享关于风险的信息。

注 1：来源：GB/T 23694—2013。

注 2：风险信息可能涉及风险的存在、性质、形式、概率、严重程度、可接受性、处理或其他方面。

3.54

风险准则　risk criteria

评价风险重要性的依据。

注 1：风险准则的确定需要基于组织的目标、外部环境和内部环境。

注 2：风险准则可以源自标准、法律、政策和其他要求。

[来源：GB/T 23694—2013，4.3.1.3]

3.55

风险管理 risk management

在风险方面，指导和控制组织的协调活动。

注：风险管理通常包括风险评价、风险应对、风险接受和风险交流。

[来源：GB/T 23694—2013，3.1]

3.56

风险降低 risk reduction

为降低风险可能性、负面后果或两者而采取的行动。

注：来源 GB/T 23694—2013。

3.57

风险分担（转移） risk sharing（transfer）

涉及与其他各方就风险分配达成协议的风险应对形式。

注 1：法律法规可能会限制、禁止或强制进行风险分担。

注 2：风险分担能通过保险或其他合同形式实现。

注 3：风险面分配程度取决于分担方案的可信性和透明度。

注 4：风险转移是风险分担的一种形式。

[来源：GB/T 23694—2013，4.8.1.3]

3.58

风险容忍 risk tolerance

组织或利益相关者为实现目标在风险应对之后承担风险的意愿。

注：风险容忍可能受到法律法规要求的影响。

[来源：GB/T 23694—2013，4.7.1.3]

3.59

风险应对 risk treatment

处理风险的过程。

注 1：风险应对可以包括：

——不开始或不再继续导致风险的行动，以规避风险；

——为寻求机会而承担或增加风险；

——消除风险源；

——改变可能性；

——改变后果；

——与其他各方分担风险（包括合同和风险融资），慎重考虑后决定保留风险。

注 2：针对负面后果的风险应对有时指“风险缓解”“风险消除”“风险预防”“风险降低”等。

注 3：风险应对可能会产生新的风险或改变现有风险。

[来源：GB/T 23694—2013，4.8.1]

3.60

安全性 security

保护不受危险、威胁、风险或损失的情况。

注：一般来说，安全性的概念是一个类似于安全可靠。两者的区别是一个强调保护不受外来危险。

3.61

安全方面 security aspects

能够减少无意、有意和自然导致危机和灾害的风险的特性、要素或性能，这些危机和灾害干扰并影响了组织及其利益相关方的产品和服务、运营、关键资产和连续性。

3.62

来源 source

任何可能单独和共同引起风险的事物。

注 1：根据 GB/T 23694—2013，定义 4.5.1.2 修改。

注 2：风险源可能是有形的或无形的。

3.63

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

可以影响、被影响或自认为会被某一决策或行动影响的个人或组织。

注 1：该术语包括与组织及其活动及成就相关的个人和团体，例如客户、顾客、合作伙伴、员工、股东、业主、销售商、地方社区、第一响应人、政府组织和监管组织。

注 2：决策者能是利益相关方。

[来源：GB/T 23694—2013，4.2.1.1，有修改]

3.64

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：供应链能包括销售商、生产设施、物流供应商、内部集散中心、经销商、批发商和其他通向最终用户的实体。

[来源：ISO 28000:2007，3.9]

3.65

目标 target

适用于组织（或其下属部门）的具体业绩要求，需根据目的进行具体设置并遵守，以实现目的。

注：根据 ISO 14001:2004，定义 3.12 修改。

3.66

测试 testing

为评估计划对于特定目标或测量标准的有效性或能力而开展的活动。

注：测试通常包括保持团队和员工有效履行其职责的演练，并显示准备和响应/连续性/恢复计划的脆弱点。

3.67

威胁 threat

可能导致意外事故的潜在原因，进而会对个人、资产、系统或组织、环境或团体造成伤害。

3.68

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。

3.69

脆弱性 vulnerability

易受风险源影响的内在特性。

[来源：GB/T 23694—2013，4.6.1.6]

3.70

脆弱性评价 vulnerability assessment

确定和量化脆弱点的过程。

4 包含韧性方针的管理体系要求

4.1 总体要求

图 4 是包含韧性方针的管理体系的流程图。

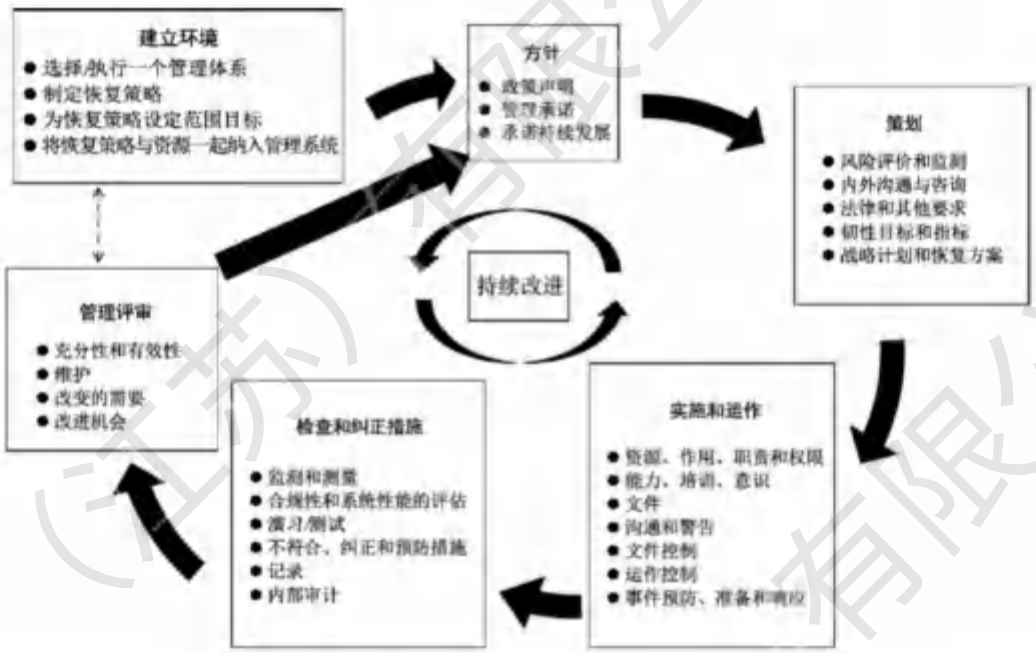

图 4　包含韧性方针的管理体系流程图

组织应根据本文件的要求制定供应链韧性方针。为实现本方针的有效性，宜将其整合在管理体系中。如在采用管理体系时，已经提出了与本文件要求相同的要求，所涉要求无需再次重复。

4.2　理解组织及其环境

4.2.1　组织应确定并详细记录其内部和外部环境。

a）　外部环境，包括：

1）　文化、政治、社会、法律、监管、金融、技术、经济、自然和竞争环境（国际、国内、地区或当地）；

2）　供应链层级、承诺和关系；

3）　影响组织目标的关键驱动因素和趋势；

4）　外部利益相关方的理解和价值。

b）　内部环境，包括：

1）　资产、活动、职能、服务、产品、合作关系、供应链和利益相关方关系；

2）　根据资源和知识（例如资本、时间、人员、流程、体系和技术）理解的能力；

3）　信息系统、信息流和决策过程（正式和非正式）；

4）　内部利益相关方；

5）　方针、目标和实现目标的策略；

6）　认知、价值和文化；

7）　组织采用的标准和参考模型；

8）　架构（如管理、角色和职责）。

4.2.2　组织在确定管理体系的环境和承诺在组织的特定内外环境下管理风险和韧性时，应识别并记录以下内容：

a）　组织的关键活动、职能、服务、产品、合作关系、供应链、利益相关方关系以及与其一个或多个供应链中的中断事件相关的潜在影响；

b) 端对端产品或服务供应链的组成部分，展示它们如何被配置或连接以提供关键产品或服务；
c) 韧性管理方针与组织目标和其他方针之间的联系；
d) 组织管理风险和韧性的基本原理；
e) 管理风险和韧性的职责和责任；
f) 组织的风险偏好或风险规避；
g) 可用于协助负责管理风险和韧性的人员的资源；
h) 承诺定期评审和验证韧性管理方针和框架；
i) 持续改进。

4.3 韧性管理方针范围

组织应在其特定内外环境下识别和记录其韧性管理方针的目标和范围。

在确定范围时，组织应做到：

a) 将纳入组织韧性方针范围的组织界限条件，一个或多个组成部分，或一个或多个端对端产品的部件或服务供应链流；
b) 制定韧性管理的要求，考虑组织的目标、目的、内部和外部义务（包括与利益相关方有关的义务）和法律责任；
c) 考虑关键的运作目标、资产、活动、功能、服务和产品；
d) 根据潜在的内部和外部干扰确定风险，这些风险可能会对组织在其潜在可能性和影响范围内的运行和职能产生不利影响；
e) 从持续改进的角度确定适应组织规模、性质和复杂性的韧性管理方针范围。

组织应确定保护和保持组织及其供应链完整性的范围，包括与利益相关方的关系，与关键供应商、外包合作伙伴和其他利益相关方的相互作用（例如组织的供应链合作伙伴和供应商、顾客、股东、其运行所在的社区等）。

根据风险评估，组织还应在开发管理体系时在安全管理、准备、减缓、危机管理、应急管理、业务连续性管理、灾害管理和恢复管理等方面分配策略权重。

4.4 韧性管理方针的资源供应

管理者应确保为执行和控制韧性管理方针提供必需的资源。资源包括人力资源和专业技能、设备、内部基础设施、技术、信息、情报和财务资源。

4.5 韧性管理方针

最高管理者应为组织的管理体系确定、记录和提供资源，并将韧性管理方针纳入其中，反映对保护人类、环境和物质资源的承诺；预测并为潜在的不良事件以及业务和运作恢复做准备。

4.6 韧性方针声明

采用本文件的组织应制定一份韧性方针声明，声明将韧性方针纳入其管理体系。韧性方针声明应适合于组织活动、职能、产品、服务和供应链的潜在威胁、危害、风险和影响（后果）的性质和规模。

该方针应：

a) 包括向员工和社区做出生命安全第一的承诺；
b) 包括持续改进的承诺；
c) 包括加强组织和供应链的可连续性和韧性的承诺；

d) 包括适应和主动风险最小化的承诺；

e) 包括遵守适用的法律要求和组织应遵守的其他要求的承诺；

f) 确定并记录与管理方针范围风险接受力，解决并指明组织采用的管理体系中与处理韧性管理相关的以下内容：

g) 制定和评审韧性管理方针目标和目的的框架：

1) 限制和例外情况参考，

2) 指定的方针负责人或负责的联系人，

3) 如何记录、执行和保持，

4) 如何传达给该组织所有的或代表该组织的专门人员，

5) 如何提供给利益相关方。

注：组织能选择公开其方针的非机密文件，不包括敏感的安全相关信息；

——如何定期接受评审和在出现重大变化时接受评审；

——如何获得最高管理者的支持。

附 录 A
（资料性）
关于将本文件纳入管理标准的参考指南

A.1 概述

采用本文件的各组织需要将韧性管理方针纳入基于 PDCA 模式的管理体系中。韧性管理方针可能是组织在制定整体管理方针时采用的众多方针中的一项。韧性管理方针将会被输入组织的管理体系中。有关每项公司管理方针的文件、执行、资源需求和执行管理应记录在认可的管理体系中。本附录提供了关于将韧性管理方针要素纳入 PDCA 型管理体系的参考指南。如果其他方针也正被纳入该管理体系，则宜寻求其他适用指南。

A.2 韧性管理方针

宜按照本文件制定、记录韧性管理方针并将其添加至整体管理体系中相应的方针部分。

A.3 管理承诺

管理者宜通过下列方式证明其在韧性管理方针的制定、执行、运行、监视、评审，保持和改进方面的承诺：

a) 制定韧性管理方针；
b) 确保制定相应的韧性管理方针目标和计划；
c) 制定有关韧性管理职能的角色、职责和能力；
d) 指定一人或多人负责韧性管理方针并授予其适当职权和能力，以对管理体系的执行和保持情况负责；
e) 向组织传达实现韧性管理目标、遵守韧性管理方针、履行法律规定韧性管理方针的职责以及持续改进该方针的重要性；
f) 提供充足的资源，用于制定、执行、运行、监视、评审、保持和改进韧性管理方针；
g) 确定风险接受标准和风险的可接受水平；
h) 确保进行内部韧性管理方针审核；
i) 对韧性管理方针进行管理评审；
j) 证明其持续改进的承诺。

A.4 策划

A.4.1 风险评估和监视

组织宜制定、执行和保持正式的文件化风险评价过程：

a) 识别有意、无意和自然造成的可能直接或间接影响下列各项的危险和威胁所造成的风险：组织的活动、运营、职能和供应链，人力资产、无形资产和物质资源，环境，其利益相关方；
b) 系统地分析风险（包括可能性、脆弱性、关键性和影响/后果）；
c) 确定对活动、职能、服务、产品、供应链、利益相关方关系和环境有重大影响的各类风险；
d) 系统评估并优先考虑风险控制、风险应对及其相关成本。

组织宜：

a) 视情况记录并保存最新资料和机密；
b) 定期评审韧性管理范围、方针和风险评价，确定其是否仍然适用于组织的内外环境；
c) 确保在制定、执行及运行韧性管理体系时考虑了主要风险；
d) 重新评估组织内部变化或组织运营环境、程序、职能、服务、合作关系及供应链改变环境中的风险；
e) 制定用于评估风险重要性的风险准则，该风险准则反映了组织的内外环境，包括其价值、目标和资源；
f) 针对最大允许停工时间、恢复时间目标以及与组织及其供应链的产品、服务和职能相关的损失的可接受水平制定标准；
g) 针对组织内部和整个供应链的活动和职能制定优先恢复时间表；
h) 评估各方案的直接和间接收益和成本，以降低风险并增强可连续性和韧性。

A.4.2 内外沟通与咨询

组织宜在风险评价过程中与利益相关方和供应链合作伙伴一同制定、执行并保持正式的文件化沟通与咨询过程，以确保：

a) 充分识别风险；
b) 了解利益相关方的利益，以及供应链中的相关性和联系；
c) 对接韧性风险评价过程与其他管理专业；
d) 依据与组织及其供应链有关的内外环境和参数进行风险评价。

A.4.3 对风险评价过程的监视与评审

组织宜制定、执行和保持正式的文件化过程，以监视、评审风险评价过程，从而：

a) 按需更新风险评价内容；
b) 确定和评估对因内外情况而可能随时间发生变化的环境、假设条件和其他因素对风险评价的影响；
c) 评估风险控制和处理的有效性；
d) 评估事故后的实际有效性。

A.4.4 法律及其他要求

组织宜制定程序并对其进行保持，以：

a) 确定组织认为与涉及组织设施、活动、职能、产品、服务、供应链、环境和利益相关方的组织危险、威胁和风险有关的法律、法规和其他要求；
b) 确定这些要求适用于组织危险、威胁、风险及其潜在影响的方式。

组织宜记录并保存最新相关信息。

组织宜确保在制定、执行和保持其韧性管理体系时考虑了组织认可的适用法律、法规和其他要求。

A.4.5 韧性目标和目的

为避免、预防、阻止、减缓、应对中断性事件并从中得以恢复，组织宜制定、执行并保持文件化目标和目的用于风险管理。文件化目标和目的宜针对组织及其供应链确立对于任务完成性、产品和服务交付情况以及职能运作十分关键的内外期望目标。

韧性目标宜来源于韧性管理方针和风险评估并与二者相一致，且包括下列承诺：

a) 通过降低可能性和后果将风险降到最低；
b) 通过采用具有适应性、主动性和被动性的方法以及财务、运营及业务要求(包括供应链承诺)来提高韧性；
c) 遵守法律及其他要求；
d) 持续改进。

在建立和评审其目标和目的时，组织宜考虑：法律、法规和其他要求；其重大风险；其技术方案；其财务、运营和业务要求；利益相关方和其他相关方的意见。

韧性目标应可经定性和/或定量衡量并宜来源于韧性管理方针且与宜其相一致，此外还宜：

a) 达到适当的细化程度；
b) 与风险评价和组织的恢复时间表相匹配；
c) 符合具体性、可测量性、可实现性、相关性和时限性原则(若可行)；
d) 传达给所有相关人员及第三方，包括分包商和供应链合作伙伴，以便其知道自身义务；
e) 定期评审，以确保与韧性管理方针目标具有相关性和一致性；并对目标进行相应修改。

A.4.6 韧性战略计划和方案

组织宜制定、执行和保持一项或多项韧性战略方案，以实现其韧性目标和目的。宜对这些战略方案进行优化并确定其优先次序，以便控制和处理与组织及其供应链发生中断的可能性和影响相关的风险。此类方案宜包括：

a) 为实现组织相关职能和层级方面的目标和目的指定职责和资源；
b) 考虑其活动、职能、法规或法律要求、合同义务和供应链义务、利益相关方的需求、互助协议和环境；
c) 实现韧性管理目标和目的所需方法、时间表和资源配置。

组织宜针对下列各项建立并保持一项或多项战略计划和方案。

a) 预防和保护——避免、消除、阻止、保护或预防中断性事件及其后果发生的可能性，包括转移处于危险中的人员或物质资源。
b) 减缓——最大限度地减少中断性事件的影响。
c) 响应——对中断性事件的初始响应，通常涉及保护人员和财产免受直接伤害。管理者的最初反应可作为组织第一响应的组成部分。
d) 连续性——提供程序、管理措施和资源，以确保组织继续满足其关键业务和运营目标。
e) 恢复——重新构建组织的各项流程、资源和能力，以便在目标规定时限内满足正在进行的工作要求。

组织宜对自身战略方案进行评估，以确定这些措施是否带来了新的风险；宜对韧性管理方案进行定期评审，以确保方案持续有效且符合韧性目标和目的；必要时，还宜对方案进行相应修改。

A.5 实施与运作

A.5.1 韧性管理的资源、角色、职责与权力

宜对角色、职责与权力进行定义、记录和传达，以便促进有效的韧性管理，并宜与实现韧性管理方针、目标、目标和方案相一致。

组织的最高管理者宜指定具体的管理代表；不论管理代表的其他职责如何，宜具有以下角色、职责和权力：

a) 确保按照本文件的要求制定、传达、执行和保持韧性管理方针；
b) 确定和监视组织的供应链合作伙伴和利益相关方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；
c) 确保能够获取足够的资源；
d) 向最高管理者报告韧性管理方针的效果以供评审并将其作为改进的依据。

组织宜建立：

a) 具有确定角色、适当权力和充足资源以监督事故预防、准备、响应和恢复情况的韧性管理团队，危机管理团队和响应团队；
b) 后勤保障和程序，用于定位、获取、存储、分发、保持、测试和解释为支持韧性管理体系生产或提供的服务、人员、资源、材料和设施；
c) 有关响应时间、人员、设备、培训、设施、资金、保险、责任控制、专业知识和材料的管理目标，以及需要从组织资源和任何合作单位获取该类资源的时间表；
d) 利益相关方进行协助、沟通、战略联盟和互助的程序。

组织宜制定财务和管理程序，以支持事故发生前、发生期间和发生后的韧性管理方针。此类程序宜：

a) 得以建立以确保推进财政决策；
b) 与已确立的权限等级和会计原则相一致。

A.5.2 能力，培训和意识

组织宜确保任何可能预防、引发、应对、减缓重大危险、威胁和风险影响或可能受其影响的人员都有能力(根据适当的教育、培训或经验)执行任务，并宜保留相关记录。

组织宜在本组织及其供应链以内确定有关管理其危险、威胁和风险及其韧性管理方针的能力和培训需求，还宜提供培训或采取其他行动来满足这些需求，并宜保留相关记录。

组织宜建立，执行和保持相关程序，以确保其所有工作人员或代表人员都能意识到该程序：

a) 重大危险、威胁和风险、与组织工作相关的实际影响或潜在影响以及提高个人业绩的益处；
b) 用于事故预防、阻止、减缓、自保护、疏散、响应、连续性和恢复的各个程序；
c) 有合格的韧性管理方针及程序和合格的供应链安全管理体系要求十分重要；
d) 自身在达到韧性管理方针合格要求方面的角色和职责；
e) 违背规定程序的潜在后果；
f) 提高个人业绩的益处。

组织宜在本组织和供应链内部建立、发扬和灌输韧性管理文化，从而：

a) 确保韧性管理文化成为组织和供应链核心价值观与组织管理方法的一部分；
b) 让供应链合作伙伴和利益相关方了解韧性管理方针以及他们在各项计划中的角色。

A.5.3 沟通与警告

关于其危险、威胁、风险和韧性管理方针，组织宜建立、执行和保持一项或多项程序，宜：

a) 记录、登记和传达文件、计划、程序、管理体系以及评估和评审结果中的各项变更情况；
b) 组织各级和职能部门之间的内部沟通；
c) 与供应链的合作单位及其他利益相关方进行的外部沟通；
d) 接收、记录和响应来自外部利益相关方的沟通信息；
e) 将国家/地区风险或威胁咨询系统/等效系统进行修改，使其融入自身规划和运营；

f) 与其供应链和其他合作单位以及利益相关方进行情报共享；

g) 提醒可能受到潜在、实际或即将发生的中断性事件影响的利益相关方和供应链合作伙伴；

h) 保证在危机和中断期间沟通工具的可用性；

i) 促进与即时响应人员和紧急响应人员之间的结构化沟通；

j) 保证多方响应组织和人员的协同工作能力；

k) 记录与事件、采取的行动和做出的决策有关的重要信息；

l) 运行沟通设施。

组织宜以生命安全为第一要务，经与供应链合作伙伴和利益相关方协商后，决定是否就重大风险进行外部沟通并记录其决策。如果决定进行外部沟通，则组织宜制定并执行外部沟通、提醒和警告方法（包括与媒体之间的沟通）。

宜定期对韧性管理方针通信系统进行测试。

A.5.4 文件

韧性管理方针文件宜包括：

a) 韧性管理方针、目标和目的；

b) 韧性管理方针的范围说明；

c) 有关韧性管理方针的主要要素及其与相关文件整合情况的说明；

d) 本文件中规定的文件（包括记录）；

e) 组织确定的必要文件（包括记录），用以确保涉及其重大风险的各项流程的有效规划、运行和控制。

组织宜确定信息的安全敏感性，并宜采取适当措施预防未经授权的信息访问。

A.5.5 文件管理

宜对韧性管理方针中规定的文件进行管理。记录是一种特殊类型的文件，宜按照 A.5.4 中的要求进行管理。

组织宜建立、执行和保持相关程序，以：

a) 符合法律法规要求；

b) 在发布前对文件充分性进行审批；

c) 必要时对文件进行评审、更新和重新审批；

d) 确保文件的变更情况及当前修订状态通过确认；

e) 确保在使用地点提供适用文件的相关版本；

f) 建立文件保存、归档和销毁参数；

g) 确保文件内容清晰易读；

h) 确保本组织认为对韧性管理方针的规划与运行所必需的外部文件是经过认定的且其文件分发处于受控状态；

i) 确认组织需要保留的所有过期文件已作废；

j) 确保文件的完整性，包括防止文件被篡改、安全备份、只有授权人员才能使用、防止损坏、磨损或丢失。

A.5.6 运作控制

组织宜明确各项必要运作和活动以满足下列要求：

a) 制定韧性管理方针；
b) 控制具有重大风险的各项活动；
c) 遵守法律法规要求；
d) 实现韧性管理方针目标；
e) 履行韧性管理方针方案；
f) 达到所需供应链韧性等级。

组织宜通过以下措施针对下列运作制定并贯彻执行适应性和主动计划和程序，这些运作包括与已确定重大风险相关，并符合其韧性管理方针、风险评价、供应链要求、目标和目的的运作，以确保这些运作在使风险最小化的特定条件下进行：

a) 制定并贯彻执行与组织活动、职能、产品和服务相关的已识别危害、威胁和风险相关的程序，并将适用的程序和要求传达给其供应链和承包商；
b) 制定并贯彻执行文件化程序，以控制因此类文件化程序缺失而导致无法满足韧性管理方针、目标和目的的情况；
c) 评估上游和下游供应链活动中的任何风险，以制定并贯彻执行文件化程序，最终使紧急情况发生的可能性降至最低和/或减轻其后果；
d) 针对影响韧性的商品和服务制定并执行相关要求，并告知各供应商。
e) 在文件化程序中规定运作标准。

这些程序宜适当包括对设备、物流、仪器等的韧性相关项目的设计、安装、运作、维修的控制。在改进现有布局或引入新布局时，如果可能会对韧性管理运作和活动产生影响，则组织宜在执行之前考虑到相关风险。有待考虑的新布局或改进后布局宜包括：

a) 改进后组织结构、角色或职责；
b) 改进后弹性方针、目标、目的或计划；
c) 改进后流程和程序；
d) 引入新型基础设施和安全设备或技术(可包括软件或硬件)；
e) 根据具体情况引入新承包商、供应商、供应链合作伙伴或人员。

运作控制过程宜：

a) 重点关注可能受到紧急情况影响的可靠性和韧性、人员安全健康和财产及环境保护；
b) 确定风险应对和控制措施(内部和外部)的负责人；
c) 确保理解能力计划中的需求信号；
d) 确保设有流程来验证供应商的响应(例如验证现场/流程/产品恢复时间)；
e) 与供应链韧性目标相匹配且适用；
f) 建立反馈回路来了解此前的风险控制方针是否发生改变，作为常规工程或流程变更或供应商决策的一部分。

A.5.7 事故预防、准备和响应

A.5.7.1 概述

组织宜制定并贯彻执行相应程序来应对可能对组织及其活动、功能、服务、供应链、利益相关方和环境产生影响的突发性事故。程序宜包含组织如何就突发性事故进行预防、防范、准备、减缓、应对和恢复

工作。为预防突发性事故，使其发生的可能性降至最低或减缓相关不利后果，组织宜针对突发性事故做好准备，并应对实际突发性事故。

当制定并贯彻执行相应程序，以便针对突发性事故进行预防、做好准备并迅速响应时，组织宜考虑采取下列措施：

a) 保护生命安全；

b) 保护资产；

c) 防止突发性事故进一步升级；

d) 缩短业务中断的时间；

e) 恢复关键业务的连续性；

f) 恢复正常运作(包括评估改进措施)；

g) 保护形象和声誉(包括媒体报道和与利益相关方的关系)。

组织宜定期进行检查，事故预防、准备、响应和恢复程序，并在必要时对其进行修改——特别是在演练后或发生可能升级为紧急情况、危机或灾害的事故或事件后。

组织宜确保任何负责事故预防、保护、准备、减缓、响应和恢复措施的人，都宜具有相应的教育背景、受过培训或具有相关经验，足以胜任其职，并保留了相关记录。

组织宜记录人员相关履历信息，并定期或在信息出现变更时对其进行更新。

A.5.7.2 事故预防、准备和响应结构

组织宜制定并贯彻执行程序和管理结构，以使具有必要权限、经验和能力的人员来预防、准备、减轻和应对紧急情况。

预防、准备和响应结构宜帮助人员开展下列工作：

a) 确认紧急情况的性质和程度，或事件可能对组织及其供应链和利益相关方造成的潜在影响；

b) 触发适当的主动或被动措施；

c) 制定关于预防、准备和应对措施的激活、运作、协调和沟通的计划、流程和程序；

d) 获取可用资源来支持应对紧急情况的计划、流程和程序，或在影响出现之前将其降至最低的工作；

e) 与供应链合作伙伴、利益相关方和地方当局以及媒体进行沟通。

A.5.7.3 事故预防、保护和减缓

组织宜制定并贯彻执行相应程序，以防止、防范和减缓紧急情况，并根据通过风险评价过程制定的恢复目标继续其活动。程序宜基于具有优先次序和层次组织的控制措施，用于选择和管理风险暴露，包括实现以下目的的程序：

a) 通过完全消除风险暴露来消除风险；

b) 通过更改活动、流程、设备或材料来降低风险；

c) 将资产与风险隔离或分离；

d) 利用工程控制来检测、阻止和推迟潜在危害或威胁因素；

e) 行政控制，如降低风险的工作实践或程序；

f) 如果无法消除或降低风险，则保护资产。

A.5.7.4 事故响应

组织宜制定并贯彻执行相应程序，以应对紧急情况，并根据通过风险评价过程制定的恢复目标维续其活动。组织宜记录相应程序(包括供应链布局)，以确保活动的连续性和对紧急情况的应对。程序宜：

a) 具体说明在中断期间宜立即采取的步骤；
b) 灵活应对意外事故和不断变化的内部和外部条件；
c) 集中处理可能破坏运作而非特定事件的各种危险和威胁的影响；
d) 根据有效假设和相关性分析制定；
e) 通过执行适当的减缓计划，有效减轻后果；
f) 考虑利用有助于恢复运作的事故后管理进行过渡。

A.5.7.5 事故连续性和恢复计划

组织宜根据管理部门批准的恢复目标制定文件化程序，详细说明组织将如何应对紧急情况，如何恢复或维持其活动至预先设定的水平。

各计划宜确定下列内容：

a) 目的与范围；
b) 成功的目标和措施；
c) 执行程序；
d) 角色、职责和权限；
e) 沟通要求和程序；
f) 内部和外部相关性和相互作用；
g) 资源要求；
h) 信息流和记录流程。

组织宜定期测试、评审并在必要时修订其连续性和恢复计划，特别是在发生紧急情况及其相关的事后评审之后。

A.6 检查和纠正措施

A.6.1 概述

组织宜通过定期评估、测试、事故后报告、经验教训，绩效评估和演练来评估韧性管理计划、程序和能力。同时，如果上述因素发生任何重大变化，宜立即在相关程序中予以说明。

组织宜记录好定期评估结果。

A.6.2 监视与测量

组织宜制定并贯彻执行绩效目标和程序，定期监视与测量对其绩效(包括合作关系和供应链关系)有重大影响的运作的特征。程序宜包括通过记录信息来监视绩效、适用的运作控制以及与组织韧性管理的合格目标和目的。

组织宜评估和记录保护其资产、通信和信息系统的体系的绩效。

A.6.3 合规性与系统绩效评估

A.6.3.1 合规性评估

组织宜根据其合规性承诺，制定并贯彻执行相应程序，以定期评估是否符合适用法律法规的要求。

组织宜评估自身是否符合应遵守的其他要求，包括行业最佳实践。组织可将此项评估与上述法律合规性评估相结合，也可制定单独程序。

组织宜记录好定期评估结果。

A.6.3.2 演练和测试

组织宜测试和评估其韧性管理方针、计划、流程和程序(包括合伙关系和供应链关系)的合理性和有效性。

组织用来验证其韧性管理方针的演练和测试宜符合下列条件：

a) 与组织的韧性管理体系范围和目标一致；

b) 以风险评估为基础，并且经过周密计划且目标明确；

c) 最大限度地降低运作中断风险以及对运作和资产造成风险的可能性；

d) 编制正式的问题后报告，报告应包含结果、建议和安排，以及时执行改进；

e) 在结合推动持续改进目的情况下进行评审；

f) 按照组织管理者确定的时间间隔定期或偶尔不定期进行，以及在组织内部和组织环境发生重大变化时进行。

A.6.4 不合格、纠正措施和预防措施

组织宜制定并贯彻执行处理实际和潜在不合格的程序及采取纠正措施和预防措施的程序。程序宜规定以下要求：

a) 识别和纠正不合格，并采取措施来减轻其影响；

b) 调查不合格，确定其原因并采取措施，以避免不合格再次出现；

c) 评估是否需要采取措施来预防不符合，并执行适当措施以避免不合格再次出现；

d) 执行纠正措施和预防措施；

e) 记录所采取的纠正措施和预防措施的效果；

f) 评审所采取的纠正措施和预防措施的有效性。

所采取的措施宜与潜在问题的影响相对应，且宜迅速执行。

组织宜识别变化的风险，并识别预防措施要求，重点关注出现重大变化的风险。

宜根据风险评估结果确定预防措施的优先顺序。

如有必要，组织宜对韧性管理方针文件进行更改。

A.6.5 记录控制

组织宜做好记录并保存记录结果，用以证明与其合格的韧性管理方针要求及实现的效果。

组织宜制定并贯彻执行相应程序，来保护记录的完整性，包括记录的使用、识别、储存、保护、检索、保留及销毁。

各记录宜清晰可辨，且可供检索。

A.6.6 内部审核

组织宜定期或偶尔不定期(由组织管理者确定)进行韧性管理体系内部审核，以确定其韧性管理方针控制目标、控制措施、流程和程序是否符合下列要求：

a) 符合本文件和相关法律法规的要求；

b) 符合组织的风险管理要求；

c) 是否有效贯彻执行并跟进；

d) 按预期计划执行。

审核程序的规划宜考虑流程的状态和重要性、待审核领域和先前的审核结果。宜明确审核标准、范围、频率和方法。挑选审核员和执行审核时，宜确保审核过程的客观性和公正性。审核员不宜对自己的工作执行审核。

宜在文件化程序中规定有关审核规划和执行及结果报告和记录保存(见 A.6.5)的职责和要求。

负责审核领域的管理人员宜确保及时采取必要的改正措施(不得无故拖延)，以消除发现的不合格项及其产生原因。后续活动宜包括验证所采取的措施和报告验证结果。

A.7 管理评审

A.7.1 概述

管理者宜定期对组织的安全管理体系进行总体评审，以确保该体系的持续适用性、充分性和有效性。评审宜包括评价管理体系的改进时机和变更需求(包括韧性管理体系方针和目标)。评审结果宜予以清楚记录，并保存记录(见 A.6.5)。

A.7.2 评审输入

管理评审输入宜包括下列各项：

a) 韧性管理体系方针的审核和评审结果；

b) 利益相关方的反馈；

c) 可用于组织内提高韧性管理体系绩效和有效性的技术、产品或程序；

d) 预防和纠正措施的状况；

e) 演练和测试的结果；

f) 先前风险评价中未充分阐明的弱点或威胁；

g) 有效性测定结果；

h) 先前管理评审工作的跟进；

i) 可能影响韧性管理方针的任何变化；

j) 方针和目标的适当性；

k) 改进建议。

A.7.3 评审输出

管理评审输出宜包括与以下方面相关的任何决策和措施。

a) 提高管理方针的有效性。

b) 更新风险评估、事故准备和响应计划。

c) 必要时修改对风险有影响的程序和控制措施，以应对可能影响韧性管理方针的内部或外部事件，其中包括对以下方面的更改：

1) 商业和运作要求；

2) 风险降低和安全要求；

3) 影响现有运作要求的运作条件流程；

4) 法律或法规要求；

5) 合同义务；

6) 风险等级和/或风险验收标准。

d) 资源需求。

e) 衡量控制措施有效性方法的提高。

A.7.4 跟进

最高管理者宜建立明确的文件化管理体系跟进方案，以确保对组织有影响的任何内部或外部有关韧性管理方针的变更得到评审。宜识别需要包含在韧性管理跟进方案中的任何新的关键活动。

A.7.5 持续改进

组织宜通过运用韧性管理方针、目标、审核结果、监视活动分析、纠正和预防措施及管理评审等方法，不断提高管理体系的有效性。

附 录 B
（资料性）
有关本文件使用的参考指南

B.1 引言

注：本附录所提供附加文件仅供参考，为本文件相关章节提供辅助性说明。本资料阐明并符合本文件相关章节要求的同时，不对其进行任何添加、删减或修改。

历史证明，自然灾害、环境事故、技术故障和人为危机之类的中断性事件时有发生，并对国营与私营企业都会产生影响，而挑战远远超出预先部署的多数应急响应计划或灾害应对工作。相关组织必须即刻投入到全面系统的灾害预防、保护、准备、减缓、响应、连续性和恢复的一系列工作中。为此，仅针对灾害或紧急情况制定响应计划还不够。今天，面对威胁，需要形成连续的、动态交互应对流程，以确保重大危机事故前、期间和过后组织核心业务的连续性。

本文件所制定的韧性方针适用于各种规模的组织，以使其达到适应性和主动降低风险的效果以及证实组织的恢复性，涉及组织实体设施、服务项目、业务、产品、供应链和运作的（业务）连续性。执行背景如下：

a) 安全风险和威胁越来越多；
b) 法律法规更加严格；
c) 商业竞争日益激烈；
d) 社会依存性（在组织、功能或管理方面）越来越高；
e) 有必要制定充分的应急响应和补救计划的意识有所加强；
f) 对利益相关方及受影响方的普遍关注；
g) 确保运作的连续性和韧性。

中断性事件得不到妥善处理可能会迅速升级为紧急情况、危机乃至灾害。做好中断性事件的预防措施，可最大程度降低其发生的可能性及影响。中断性事件不处理，除了会酿成重大人身或环境损害、损伤或死亡，还可能毁坏组织形象、声誉或品牌。

对潜在事故或中断性事件做好适应性主动规划和准备工作可降低中断性事件发生的可能性、影响及持续时间。整体的管理流程有助于避免和最大程度降低关键性服务和运作中断的可能性，因此可尽快使服务和运作恢复正常。

本文件所提供的指南或建议适用于任何需要明确最佳实践并予以开展的组织，以协助并推动其在以下方面的工作：

a) 降低其供应链各个环节的风险；
b) 从最高管理者角度为其方针制定提供远见和指南，以保护组织资产并确保其韧性；
c) 鉴定并评估资产、服务和功能，以明确运作与业务取得短期和长期成功的关键部分；
d) 识别潜在危险和威胁，并对其进行风险和影响评价；
e) 预防和/或减轻多种危险和威胁产生的影响，包括自然灾害、技术和环境事故以及人为灾害（恐怖主义和犯罪）；
f) 了解保护资产和促进其韧性所需的职责与责任；
g) 做好必然事故/紧急情况准备工作，并管理响应资源；
h) 建立方针联盟，并制定互助协议；
i) 制定并维持事故/紧急情况应对准备和响应计划及相关运作程序；

j) 制定并执行培训与演练方案，以支持和评估预防、保护、事故/紧急情况应对准备、响应计划和运作程序；

k) 制定并执行培训方案，以落实准备工作、响应计划和运作程序；

l) 确保相关员工、客户、供应商及其他利益相关方具有预防、保护、事故/紧急情况应对准备和响应一系列准备工作的意识，以及（必要时）有信心付诸执行；

m) 制定内部和外部沟通程序，包括媒体或公众要求获取信息的响应；

n) 确定考核和证实处理成功的衡量标准；

o) 记录支持关键运作功能所需的关键性资源、基础设施、任务与责任；

p) 确定相关流程，以确保所获取的信息为最新信息，且与变化的风险与运作环境相关。

本文件对于组织保护其有形、无形和人力资产方面极具价值。组织管理体系运行能否成功取决于组织各级管理者和各职能部门尤其是组织最高领导层是否尽职尽责。决策人员必须为管理体系运行所需的资源预留预算。组织有必要建立适当的管理结构并使之落实到位，以有效进行中断性事件的预防、减缓和处理工作。此举可确保所有相关人员了解谁是决策者，决策如何执行以及参与人员的角色与责任是什么。对于安排参与事故处理的人员，宜将其所承担的责任纳入其所在岗位职责范围内，而非建立在自愿基础上。无论哪类组织，其领导层都有责任制定生存计划，确保利益相关方的权益。

B.2 通用指南

管理体系是多层面的动态流程，其中，各个要素作为功能单位相互作用形成一个有机整体。体系所提供的框架基于：体系内部的各个组成部分，在彼此相互联系和与其他体系相联系而非孤立的情况下去看待，更易于理解。完全了解并执行管理体系各要素的唯一方法是结合整体去理解部分。因此，需要注意的是管理体系并非一系列事件的简单循环，而是一个复杂的组合，其各要素之间相互关联相互作用，从而形成一个循环往复的过程。在该过程中，设定好背景和相关方针后所进行的风险评价、体系执行与运行以及评估与评审工作并非只是一系列连续性步骤，而是由一系列活动相互关联而形成的有机网。

该管理体系方法具有以下特征：

——了解该体系运作的背景和环境；

——明确该体系的核心要素及体系边界；

——了解该体系内各要素角色与功能；

——了解该体系各要素间的动态互动关系。

该体系的使用能确保整体方针与方针得以制定，为方针与方针的制定提供了可靠的分析基础，以便使其在组织运行的复杂多变的环境中得以落地执行。建立好框架进行风险评价以及对方针和方针执行前和执行期间的有效性进行评估，为整个流程中的决策制定提供了反馈渠道。

本文件中所规定的组织韧性（OR）管理方针与管理体系，目的都是提高组织安全、准备、响应、连续性及韧性。因此，本文件使用的前提是组织会定期评审与评估其管理体系与韧性方针，以识别改进时机，并付诸执行。持续改进的速度、范围与时段由组织根据经济及其他情况来确定。改进管理体系旨在进一步提高安全、准备、响应、连续性、恢复状况及组织的韧性。本文件对组织有以下要求：

a) 制定合理的韧性管理方针；

b) 结合组织过去、现在或计划中的活动、功能、产品和服务识别所存在的危险和威胁，以确定具有重大意义的风险；

c) 明确适用的法律要求及组织应遵守的其他要求；

d) 确定优先顺序，设置适宜的韧性管理目标和目的；

e) 建立用来执行方针、实现目标和满足目标的体系和方案；

f) 促进规划、控制、监视、预防和纠正措施的执行以及审核和评审工作的落实，确保方针得到遵守、韧性管理体系得当；

g) 能够适应不断变化的环境。

B.3 理解组织及其环境

为了使组织能够设计和执行一个具有韧性方针的管理体系用于管理组织风险及其供应链风险，组织必须首先评估和理解其内部和外部操作环境。当在管理环境中制定韧性方针时，组织宜考虑与其本身及其供应链有关的各种内部和外部参数(见图 B.1)。环境将决定组织及其供应链的管理风险的必要范围和标准，并且决定了设定风险评估目标、风险和恢复标准，以及风险评估与风险应对参数的基础。

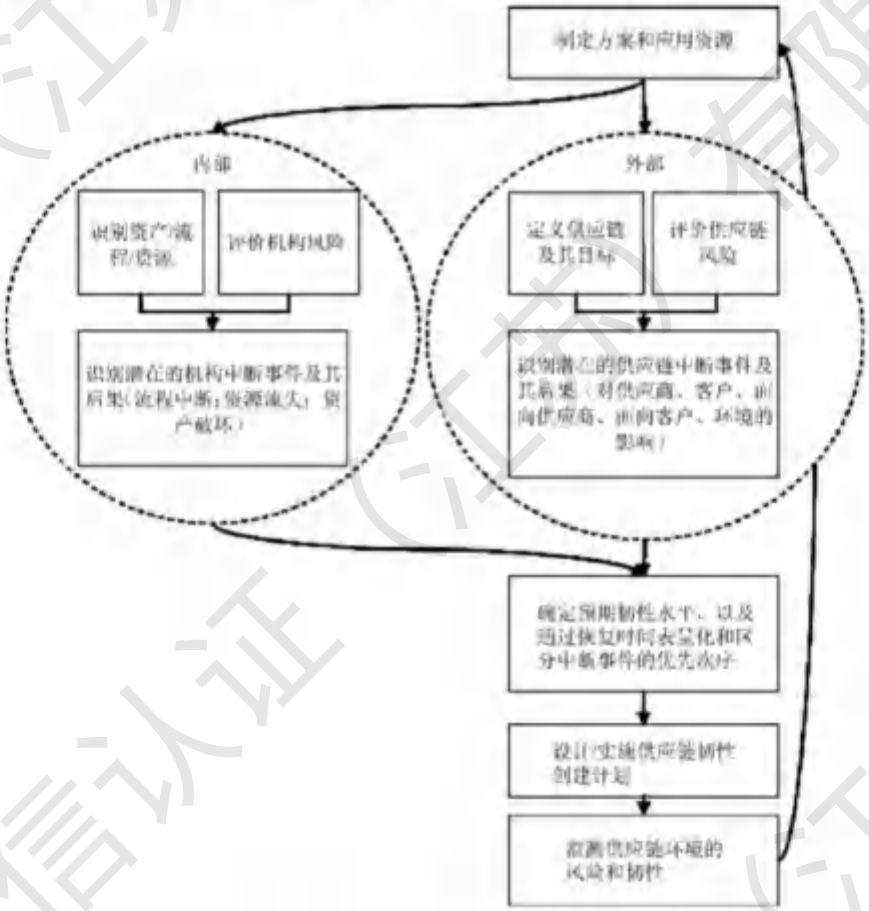

图 B.1 理解供应链韧性管理的环境

B.4 韧性管理方针的范围

组织具有定义其范围的自由度和灵活性，并且可以选择对整个组织、组织的特定运行单位、或一个或多个端到端产品或服务的供应链流程的组成部分执行本文件。组织宜定义其韧性管理方针的范围并提供文件证明。

范围化是为了阐明组织的范围和将应用韧性管理方针的供应链节点，对于大型组织在特定位置的下属组织更是如此。在定义了范围之后，韧性管理方针需要包括组织在相关范围内的所有业务、产品和服务。在设定范围期间，韧性管理方针的可靠性取决于选择的组织范围。如果组织的某个部门被排除

在其韧性管理方针的范围之外，组织应能够说明具体原因。

如果由特定运行单位执行本文件，组织其他部门制定的方针与程序在适用于特定操作单位的情况下，也可用于满足本文件的要求。

韧性管理包括中断性事件之前、期间和之后的各种问题和行动。因此，本文件涉及了预防、规避、制止、准备、减缓、响应、连续性和恢复。风险环境以及业务/操作真实性，集中于每个组成部分的不同战略权重，但是没有一个组成部分加权应为零。适用性声明宜根据风险评估(见A.4.1)说明开发管理体系期间的安全管理、准备工作、应急管理、灾害管理、危机管理和业务连续性管理。

B.5 韧性管理方针的资源供应

宜识别韧性管理方针所需的资源，其中包括人力资源和专业技能、设备、内部基础设施、技术、信息、情报和财政资源。对于制定、执行、控制和保持韧性管理方面必不可少的资源，最高管理者宜确保这些资源的可用性。

B.6 韧性管理方针

韧性管理方针是执行和改进一个组织的韧性管理体系的推动力，以便韧性管理体系可以维持和提高其可连续性和韧性。因此，韧性管理方针宜反映出最高管理者的承诺：

a) 符合适用的法律要求及其他要求；

b) 中断性事件的预防、准备和减缓措施；

c) 持续改进。

韧性管理方针可作为形成基础的框架，组织可根据基础情况设定其目标和目的。内部和外部相关方(尤其是组织的供应链合作伙伴)宜能够充分明确理解韧性管理方针，并且宜为了反映变化条件和变化信息而定期评审和修改韧性管理方针。宜能够明确识别其适用领域(范围)，并反映出各种业务、功能、产品和服务的风险的独特性质、规模和影响。

韧性管理方针宜通知到为组织工作(或代表组织)的所有人员，包括其供应链和在组织场所内工作的承包商。可以采用多种方式将方针声明通知承包商，例如准则、导则和规程，而且可能只通知方针的相关条款。对于任何更广泛的法人团体的韧性管理方针，组织的最高管理者宜在获得该团体批准的情况下，在该团体的韧性管理方针的环境中规定本组织的韧性管理方针并提供文件证明。

最重要的是组织的最高管理者赞助、提供必要的资源，并负责创建、保持、测试和执行综合的韧性管理体系。因此，最高管理者的首要任务是必须确保组织内部的各级管理者和工作人员都理解韧性管理体系。同样重要的是，最高管理者对韧性管理体系使用"自上而下"的方法，以便组织的各级管理者都了解到有义务进行有效和高效的计划保持，这是整体管理优先项目的一部分。

宜委任一个韧性管理计划团队(包括来自组织所有主要职务和支持团体的高级领导)，负责确保韧性管理体系被广泛接受。

B.7 策划

B.7.1 风险评估和监视

风险评估流程能够让决策者更好地理解可以影响实现决策者及其供应链的操作和经营目标的风险。其目的是为组织创建一个用于识别重要资产、危险、威胁、脆弱性、风险和影响的系统化流程，以便确定上述因素对组织及其供应链具有重要意义。风险评估为现有日常检查的适当性和有效性的评估提供了依据，并提供最适合用于管理和风险应对的方法的决策。识别组织的韧性管理方针宜优先解决的风险。风险评价为在安全管理体系内部设定目标、目标和计划，以及测量韧性管理的功效提供了基础。

组织宜使用 ISO 31000:2009(图 B.2)。

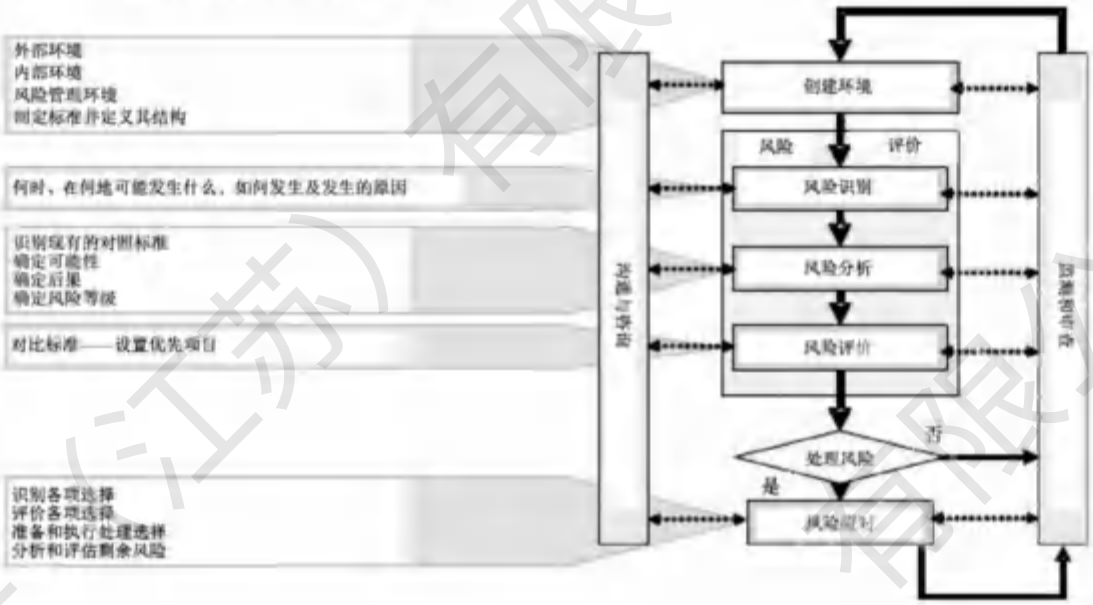

图 B.2 风险管理流程

创建一个环境,让组织确定他们认为需要保护的项目,并且为了确保一致性而定义风险评价要素的分级系统。

外部环境包括:

——(国际、国家、地方的)文化环境、政治环境、法律环境、监管环境、财务环境、自然环境、业务环境;

——影响各个目标的主要推动力和发展趋势;

——外部利益相关方的认知和价值。

内部环境包括:

——资源和知识(人员、流程、系统、技术、时间和资金)方面的已知能力;

——信息(系统、流程和决策程序);

——内部利益相关方;

——组织的目标和战略;

——认知、价值和文化;

——方针与程序;

——标准、参考模型、结构(管理、职责和义务);

——风险评价目标、风险准则[脆弱性、危险(威胁)的可能性及后果]、风险评价计划及时间安排的议定流程。

在创建内部和外部环境的过程中,组织宜全面识别本组织的所有重要资产。其中包括识别各类资产相对于组织生存能力和成功的重要性。这宜包括人员、资产、资料、流程、业务和无形资产(例如市场份额或市场地位、信誉、可信度等)。资产可包括组织已建成的建筑物和/或经营使用的重要设备。组织可选择各类业务、产品和服务用于识别其危险程度、风险和影响。

在组织的内部和外部环境中执行风险评价过程。风险评价是指风险识别、风险分析和风险评估的整个过程。

a) 风险识别：查找、识别和记录风险的过程；其中包括在识别过程中输入威胁、危险程度和脆弱性评价。此程序考虑了风险成因和来源，以及可能影响组织及其供应链的事件、情况和环境。识别似乎可能存在的威胁/危险包括提前收集与潜在危险源有关的信息资料。威胁/危险可包括但不限于人员损伤、财政因素、竞争对手或供应商的影响、业务活动或组织内部和外部的其他情况。通过脆弱性评价可以识别实际业务、程序活动及经营活动存在的脆弱性，然后可通过或利用这些脆弱性发现威胁情况。

b) 风险分析：发现和了解风险的过程。这一过程为确定宜处理哪些风险和最适当的风险应对方法提供了决策基础。同时考虑风险成因和来源、风险后果、及发生事故和相关后果的可能性。组织宜确定哪些位置或哪些设施发生的事故后果或事故影响必须视为一项威胁。这些后果可归类于人员死亡或受伤、财务或业务影响、营业中断、建筑物损坏和损坏无形资产（声誉、品牌、信誉、行业地位和社会地位）。确定后果的过程也可视为影响分析。

c) 风险评估：按照创建环境时规定的风险准则，比较估计风险水平的过程。风险评估确定了风险水平和风险类型的重要性。风险评估利用了风险分析期间获得的风险了解，然后对风险控制和风险应对做出必要的战略决策。

风险评估可帮助理解风险及其起因、后果和风险可能性。因此，组织宜在其韧性管理体系范围内进行综合风险评价，并考虑与以下各项相关（有意和无意）的输入与输出：

a) 组织当前和过去的有关业务、产品和服务（组织内部及其供应链内部）；

b) 规划发展或新发展，或新业务或改良业务、功能、产品和服务；

c) 与供应链合作伙伴和利益相关方之间的关系；

d) 与环境和社会的相互作用；

e) 关键基础设施。

这一过程宜考虑正常和异常工作条件、停工和启动条件，以及合理可预见的中断情况和紧急情况，以便设定恢复时间目标和响应恢复时间的要求。但是宜注意一点：不可能预测所有中断情况和紧急情况，因此组织还必须考虑其重要资产、业务和功能出现中断的影响（不考虑中断的性质），以便在组织内部及其供应链内部设定恢复时间目标和响应恢复时间的要求。

对于风险评价，有许多方法可用于确定分析步骤的顺序。不管采用哪种方法，组织都宜拥有一个正式且文件化的程序用于风险识别、风险分析和风险评估（包括威胁和危险识别），以及风险、脆弱性、危险程度、后果和影响分析。

风险评价宜：

a) 考虑与组织及其供应链的业务、功能、产品和服务相关的各种风险（包括危险程度），以及这些风险对组织的业务、人员、不动产、资产、赔偿、形象和声誉、利润、信誉、和/或环境产生直接或间接影响的可能性；

b) 将文件化的定量或定性方法用于评估已识别的潜在风险的可能性或概率，以及识别风险影响的重要性；

c) 以合理的标准为基础，对其业务识别的所有潜在风险加以适当考虑；

d) 考虑本组织与其他组织之间的相互依赖关系，包括关键基础设施和供应链的依赖性和义务；

e) 考虑数据和通信的完整性及网络安全；

f) 评估用于管理组织活动的法律义务及其他义务的后果；

g) 考虑与利益相关方、承包商、供应商及其他相关方有关的风险；

h) 分析与风险有关的信息，选择可能导致重大后果的风险和/或难以确定后果关键性的风险；

i) 分析和评估每项危险或威胁、每项重要资产的韧性水平；

j) 评估可控和可改变的风险和影响(然而,组织在任何情况下都要确定可控程度及应对风险接受、风险规避、风险管理、风险最小化、风险容忍、风险转移和/或风险应对的方针)。

在某些地区,关键基础设施、社会资产和文化遗产可能是组织运营所处环境的重要组成部分,因此在理解组织风险及其对周围环境的影响时宜予以考虑。

一个组织可能存在很多风险,因此为了确定组织认为的重大风险,宜制定和记录相应的标准和方法。单个方法不能确定重大风险。但是所采用的方法宜能得到一致的结果,并且包括制定和使用评估标准,例如与组织每项业务和功能、法律问题及内外利益相关方的问题相关的危险程度的评估标准。组织宜分析其业务中断的可能性及影响,并且识别需要优先恢复的重大业务,以便设定恢复时间目标。

组织在评价影响时宜考虑:

a) 人力成本:对员工、客户、供应商及其他利益相关方造成的身体伤害和心理伤害;

b) 财务成本:设备和资产重置、停工、加班费、股票贬值、滞销/业务损失、诉讼、违规罚款/处罚等;

c) 企业形象成本:名誉、社会地位、负面新闻、客户流失等;

d) 组织所在地的经济损失:间接影响地区经济、地区网络经济下滑、地方管辖组织的课税基础损失等;

e) 环境影响:环境质量退化或濒危物种减少。

对于评估最大允许停工时间、可接受的损失程度,以及优先考虑的恢复时间表,组织的目标宜以下列因素为基础:

a) 组织的供应链承诺,考虑上游和下游后果;

b) 在各种影响变得无法接受之前,这些流程的无功能状态可持续多长时间;

c) 这些流程宜在多久时间内恢复(首先恢复允许中断时间最短的流程);

d) 根据年度时间(年终、税务申报等)制定不同的恢复时间目标;

e) 识别和记录战略联盟、相互帮助、手动应急方案、通知/警报等备用程序;

f) 评估备用程序与等待系统恢复之间的成本对比。

当组织开发的信息涉及重大风险时,组织宜考虑需要保留用于历史用途的信息,以及如何将这些信息用于设计和执行其韧性管理方针。

风险的识别和评估过程宜考虑业务活动位置,开展分析的成本和时间,以及可靠资料的可用性。出于商业规划、监管或其他目的而开发的信息,也可在此过程中使用。

识别和评估风险的过程并非为了改变或增加组织的法律义务。

B.7.2 法律及其他要求

组织需要识别适用于自身业务和功能的法律要求。其中可能包括:

a) 国家和国际的法律要求;

b) 国家级/省级/部级法律要求;

c) 地方政府的法律要求。

组织可能同意的其他适用要求示例包括(如适用):

a) 与政府当局签订的协议;

b) 与客户签订的协议;

c) 非监管准则;

d) 自愿性原则或操作规程;

e) 自愿性标志或产品管理承诺;

f) 行业协会的要求;

g) 与社会团体或非政府组织签订的协议；

h) 组织或其上级组织的公开承诺；和/或

i) 企业/公司要求。

在识别这些要求的过程中，通常需要确定如何将法律要求及其他要求应用于组织的风险评价。因此，可能不需要单独或额外的程序用于上述确定工作。

B.7.3 韧性目标和目的

在切实可行的情况下，目标和目的宜具有明确性和可测量性。目标是指组织要求自身达到与方针相一致的总体目标。目标是指适用于组织(或其下属部门)的具体工作要求；目标是根据目标而进行具体设置，在实现目标时需要满足各项目标。目标和目的宜包括短期问题和长期问题。项目计划宜规定实现目标和目的的战略手段。

目标、目的和计划都宜以风险评价为基础。

在考虑技术选择时，组织宜在经济上可行，具有成本效益和判断适当的情况下考虑使用最佳可行技术。

组织的资金需要基准并不意味着组织必须使用具体的成本会计方法；然而，组织可选择考虑直接、间接和隐性成本。

B.7.4 韧性战略计划和方案

创建和使用一个或多个方案是成功执行韧性管理方针的重要步骤。每个方案宜说明组织如何实现其目标和目的，包括时间表、必要的资源，以及负责执行相关方案的人员。这些方案可能需要根据组织内部的具体工作部门进行细分。

在适当且切实可行的情况下，方案宜包括考虑组织在各个阶段涉及供应链义务、规划、设计、施工、调试、运行、翻新、产品、销售、废弃物处理和退役的业务活动和功能。可以为当前业务和新业务、产品和/或服务开展方案编制。

预防、准备和减缓方案宜考虑：转移处于危险当中的人员和财产；重新设置、改造或提供防护系统或防护设备；信息、数据、文件和网络安全；针对威胁或危险建立警告和通知程序；转移冗余或重复的(包括来自合作伙伴组织)重要人员、关键系统、设备、信息、业务或材料。

组织宜制定事故响应和恢复计划，考虑核心业务活动、供应链义务及合同义务，工作人员及周边居民的必需品、工作连续性和环境修复。组织宜有不同的危机管理方法。在出现中断性事件的情况下，不管采用哪种方法，都需要优先计划和执行三个通用且相互关联的管理响应步骤。

a) 紧急响应：对中断性事件的初始响应，通常涉及保护人员和财产免受直接伤害。管理者的最初反应可作为组织第一响应的组成部分。

b) 连续性：提供程序、管理措施和资源，以确保组织继续满足其重要业务和运营目标。

c) 恢复：重新构建组织的各项流程、资源和能力，以便满足工作要求。这通常包括引入重大的组织改进措施，甚至重新调整战略目标或运营目标。

B.8 执行与运作(战术执行)

B.8.1 资源、角色、职责与权力

韧性管理方针的成功执行需要为组织或代表组织工作的所有人员的共同努力。因此，角色和职责不宜被视为局限于风险管理功能，但也可包括组织的其他领域，例如除了风险管理、安全、准备、连续性和响应工作之外的业务管理或职能组织。

承诺宜从最高管理者开始。因此，最高管理者宜制定组织的韧性管理方针并确保这一方针的执行。作为承诺的一部分，最高管理者宜任命一名或多名管理代表，并赋予执行韧性管理方针方面的相应责任和权力。对于大型组织或复杂组织，可能需任命多名管理代表。对于中小型企业，可由单独个人承担这些职责。

在中断性事件期间，需要相应的行政组织介入方有效处理危机管理。必须明确规定管理结构，决策权力和执行职责。组织宜成立一个危机管理团队专门负责管理事故/事件响应。此团队宜包括人力资源、信息技术、设施、安全、法律、通信/媒体关系、生产、仓储及其他业务部门和主要辅助职能部门的工作人员，并且接受最高管理者或其代表的直接指挥。

危机管理团队可能配备若干个应急响应工作组，具体数量根据组织规模和类型、员工人数、位置等因素合理确定。响应工作组宜针对潜在危机的各个方面制定不同的响应计划，例如损害评价、场地恢复、工资单、人力资源、信息技术与行政支持等。各项响应计划宜保持一致，并且宜纳入整个韧性管理体系。宜根据每个人的技能、承诺水平与既得利益，招募工作人员成为响应工作组成员。

管理人员还宜提供适当的资源，确保韧性管理体系的创建、执行和保持工作。另一个重点是明确规定韧性管理体系的主要角色与职责并告知为组织或代表其工作的所有人员。

此外，与外部利益相关方合作时，宜同样明确规定相应的角色、职责和权力，形成书面文件并传达。其中宜包括承包商、合作伙伴、供应链内部组织、政府当局和金融组织之间的相互配合。

B.8.2 能力、培训和意识

组织宜识别有责任和有权代表其执行任务的所有人员所需的意识、知识、理解和技能。本文件规定了下列要求：

a) 遵守韧性管理方针和程序及合格的全面的管理体系要求的重要性；

b) 重大危险、威胁和风险，与组织工作相关的实际影响或潜在影响以及提高个人业绩的益处；

c) 组织的角色和职责需要达到合格的韧性管理方针的要求；

d) 用于事故预防、制止、减缓、自保护、疏散、响应和恢复的各个程序；

e) 违背规定程序的潜在后果。

宜为内部和外部利益相关方(包括供应链合作伙伴)制定的意识和教育方案，可能会受到中断性事件的影响。

可通过培训、教育或工作经验获得或提高各种意识、知识、理解和能力。

组织宜要求为其工作的承包商能够证明他们的雇员具有必要的能力和/或经过适当的培训。

管理人员宜确保相关人员(特别是执行特殊韧性管理职能的人员)具备必要的经验、能力和培训水平。

所有人员宜经过培训，确保能够在出现中断性事件或危机的情况下履行他们的个人职责。还宜向这些人员简要介绍韧性管理体系的主要组成部分，以及对他们产生直接影响的响应计划。相关培训可包括预防程序、保护和减缓措施、疏散、就地避难、办理员工登记手续、各周工作场所安排以及由公司处理的媒体垂询。

危机管理与响应工作组应被告知其职责和义务，包括与现场急救人员、供应链合作伙伴和利益相关方相互配合。重大行动核对表和需要收集的信息是培训和响应过程的重要手段。各个工作组宜定期进行培训(至少每年一次)，新成员宜在加入时进行培训。这些工作组还宜进行事故预防方面的培训，然后逐步提高到危机预防培训。

建议所有可能涉及各种响应(如消防、治安、公共卫生和第三方供应商)的外部资源应熟悉响应计划的相关部分。

B.8.3 沟通与警报

内部沟通对确保有效执行韧性管理体系具有重要意义。内部沟通方法可包括定期的工作组会议、业务通信、公告板和内部网站。

组织宜识别负责涉及风险评价中识别出潜在中断的情报、警报、预防、响应和恢复工作的公共部门机关、组织和官员，并与之建立联系。在正常和异常情况下，都宜做出内部和外部沟通和警报的安排。

组织宜执行来自供应链、利益相关方和其他相关方的有关沟通的接收、记录和响应程序。这一程序可包括与利益相关方进行对话及对其相关事项加以考虑。在一些情况下，对相关方的事项作出响应可能包括与组织功能和业务有关的风险和影响的相关信息。这些程序还宜解决与政府当局就制订应急计划及其他相关问题进行必要的沟通。

组织可能希望在设计沟通内容时，考虑对相关目标群体作出的决策、适当的信息和主题以及方式选择。在考虑对外沟通危险、威胁、风险、影响和控制程序等问题时，组织宜考虑到所有利益相关方的观点和信息需求。如果组织决定对外沟通危险、威胁、风险、影响和控制程序等问题，则宜制定相应的程序。此程序可根据一些因素而改变，包括将要沟通的信息类型、目标群体及组织的个别情况。外部沟通的方法可包括年度报告、业务通信、网站、警报和社区会议。

有效沟通是管理中断或危机的最重要环节。为了更好地传达警报、警告、危机和组织响应信息，宜识别所有的内外利益相关方。为了向各个群体提供最好的沟通和适当的信息，可适当地对受众进行分区管理。采用这一方法，可向单个团体发布专门定制的信息。

预规划是进行沟通的关键。对于风险评价中识别出的各种威胁，可设计相应的信息模板、脚本和声明。宜建立能够确保在短时间内发布通知信息的程序，尤其是使用内部网、互联网站点和免费热线电话等资源。

组织宜指定一位主要发言人(以及指定备选人)，负责管理和向媒体和其他人发布应急通知。此发言人宜在危机之前接受媒体方面的培训。宜通过源头统一过滤所有信息，确保发布信息的一致性。宜强调需要迅速告知所有工作人员关于在何处查询来自媒体的电话，并且只有经授权的公司发言人才能向媒体发言。在一些情况下，也可能需要经过适当培训的现场发言人。

B.8.4 文件

文件的详细程度宜足以说明韧性管理方针及各部门如何合作以及告知可从何处获取关于韧性管理方针具体执行工作的更详细信息。这些文件可与组织执行的其他管理体系的文件综合使用。文件不必局限于手册的形式。

不同组织的韧性管理方针文件具有不同的范围，原因如下：

a) 组织的规模和类型及其活动、产品或服务；
b) 流程复杂性及其相互作用；
c) 工作人员的能力。

文件示例包括：

a) 方针、目标和目的声明；
b) 有关重大风险的信息；
c) 程序；
d) 过程信息；
e) 组织结构图；
f) 内部和外部标准；

g) 现场响应计划、减缓计划、应急计划和危机计划；

h) 记录资料。

关于文件程序的任何决定宜基于下列因素：

a) 没有这样做的后果(包括对人员、物质资源和环境造成的后果)；

b) 需要证明遵守法律要求和组织认可的其他要求；

c) 需要确保活动持续进行；

d) 这样做的好处，其中包括：

1) 更容易执行沟通和培训；

2) 更容易保持和修订；

3) 降低歧义和偏差的风险；

4) 论证可能性和可见性；

e) 本文件的要求。

针对韧性管理方针之外的其他目的而创建的初始文件，也可用作本方针的一部分，而且需要在本方针中加以引用(如使用)。

B.8.5 文件管理

本条的目的是确保组织创建和保存文件的方式足够执行韧性管理体系。然而，组织的主要焦点宜集中在有效执行韧性管理体系及安全、预备、响应、连续性和恢复工作上，而非复杂的文件管理体系。

组织宜确保文件的完整性，包括防止文件被篡改、安全备份、只有授权人员才能使用、防止损坏、磨损或丢失。

B.8.6 运作管理

相关组织宜对已识别的重大风险相关的运作进行评估，确保其运作方式能控制或降低相关风险及不良后果发生的可能性，以满足韧性管理方针的要求，符合其目标和目的。评估宜包含相关运作的所有环节，包括供应链和维修活动等。

韧性管理方针的本部分内容针对如何将系统要求运用于日常运作提供指导：要求通过文件化程序进行管理，避免因缺乏文件化程序而导致偏离韧性管理方针、目标和目的。

为了尽量降低发生中断性事件的可能性，运作管理程序宜包括对设备或仪器的相关风险项目进行设计、安装、操作、翻新和修改管理。当修改现有计划或采用新计划可能对运作及活动造成影响时，组织宜在计划执行之前将相关威胁和风险降至最低。

B.8.7 事故预防、准备和响应

B.8.7.1 概述

每个组织都有责任制定适合自身特殊需要的事故预防、准备、减缓、响应和恢复程序。在制定这些程序时，组织宜考虑以下方面：

a) 宜识别、理解和应对潜在的中断性事件，以及为了避免或预防中断性事件需要采取的措施。风险评价可用于识别潜在中断性事件的详细情况，包括所有预兆和警报信号。

b) 风险管理宜为建立在正式风险评价基础上的一个系统化和整体化的过程，通过识别、测量、量化和评估风险，从而提供最佳的解决方案。

c) 风险应对方案可包括规避、消除、降低、分散、转移和接受等方针。规避和消除风险可避免能够产生风险的活动或消灭风险源。降低风险可减少风险或损失程度。分散风险是指分摊资产

和/或潜在的能力损失。转移风险是指与其他一方或多方一起分担风险。接受风险是对具体风险作出理性决断。

B.8.7.2 事故预防、准备和响应结构

组织宜建立相关程序，确认在发生重大特殊危险时是否需要采取一定的措施，以避免、预防、减缓或响应潜在的中断性事件。宜制定一个强有力的检测和规避方针与程序计划支持这一过程。

某些部门或职能对观察即将来临的危机的警告信号具有特殊意义。分配到这些部门或职能的工作人员宜经过适当培训。宜将报告潜在危机(包括通知机制)的责任明确告知所有工作人员。如果已经设立了一个良好的上报机制，而且专门关注工作人员上报的信息，工作人员群体通常也可能是预兆信息的最佳来源之一。

潜在中断性事件一旦被确认，宜立即上报至管理部门的负责人或负责危机通知及组织和供应链内部管理的其他人员。

——宜制定和记录具体的通知标准，确保所有工作人员遵守标准要求(清楚记录通知电话的时间和顺序)。实际激活响应过程宜需要满足非常特殊的条件。

——当满足潜在危机的某些条件或参数时，获得授权的工作人员宜有权接触到更新的、保密的人员和组织名单。

——宜及时、清楚地通知中断情况或危机情况，并宜使用各种程序和技术(了解所使用设备的优点和局限性)。

——在一些中断情况和危机情况下，通知系统本身也受到事故的影响，包括能力问题或基础设施损坏。因此，重点是要在通知系统中建立冗余，可通过其他不同方式联系名单上的个人和组织。

宜在中断性事件开始时进行问题评价(确定待解决问题性质的一个评估性决策过程)和关键性评价(确定中断性事件的严重程度及从长远来看可能出现所有相关后果的过程)。需要考虑的因素包括问题的关键性、问题升级的可能性，以及问题状况可能对组织及其供应链产生的影响。

宜对将要出现紧急状况或危急情况的位置进行清楚的界定和记录，并且使用非常具体的控制参数。还宜明确规定和分配宣布危机的责任。宜识别第一责任人和第二责任人。宣布将要出现紧急情况或危机情况的活动包括但不限于：

a) 通知供应链合作伙伴及其他相关方；
b) 额外电话通知；
c) 疏散、寻找避难所或重新安置；
d) 安全协议；
e) 激活响应场地和备用场地；
f) 团队部署；
g) 人员分配和可达性；
h) 激活应急协议；
i) 运营变更方案。

B.8.7.3 事故预防、保护和减缓

事故预防包括采取主动性措施在情报、执法和政府组织之间进行协调；建立信息共享协议；重要资产实物保护；访问控制；意识和准备培训计划；警告和警报系统；以及减少威胁的实际行动。

组织文化、运营计划和管理目标宜鼓励个人承担各自有关预防、规避、制止和检测的责任。

制止和检测可使针对本组织的中断行为或活动更难以执行，而如果没有产生负面影响，避免受到更

大限制。事故预防、检测和制止方针可能考虑以下内容：

a) 建筑方面：天然或人造障碍、重新设计或重新部署基础设施；

b) 运营方面：管理程序、清除危险物质、重新设计系统和操作、安全人员的后续命令、雇员意识方案、避免反监视和反情报活动、重新部署系统、操作、基础设施和人员；

c) 技术方面：替代材料和程序、可互操作的通信和信息网络、入侵检测、访问控制、记录监视、包裹和行李筛查、以及系统控制。

实体安全规划包括保护周边区域、建筑物周边、内部空间防护、以及保护资产和财产。从外部边界开始进行防护。

a) 实体安全规划宜包括检测、制止、延迟和响应等功能。

b) 宜设计实体安全措施，以便尽可能从目标开始检测。延迟设计成更接近目标。

c) 安全系统设计宜通过评价和响应连接外部或内部检测。

d) 实体安全措施可能包括：通过环境设计预防犯罪、物理屏障和场地硬化、物理进入和访问控制、警戒照明、入侵检测系统和警报、闭路电视、保安人员以及安全方针和安全程序。

宜采用成本效益减缓方针预防或减轻潜在危机的影响。

a) 减缓方针宜考虑立即行动、中期行动和长期行动。

b) 宜确定有助于减缓过程的各种资源。宜将这些资源（包括重要人员及其作用与责任、设施、技术和设备）记录在计划当中并成为"一切照旧"的一部分。

c) 按照减缓方针的要求，宜持续监视各类系统和资源。这类监视也可视为简单的库存管理。

d) 还宜持续监视可支持组织减缓危机的资源，以确保它们在中断性事件和危机期间能够使用且按计划执行。这类系统和资源的示例包括但不限于：应急设备、火灾报警器和灭火系统、本地资源和供应商、备用工作场所、地图和平面图、系统备份和异地存储。

B.8.7.4 事故响应

宜围绕实际"最坏情况"制定准备与响应计划，前提是响应范围恰好与实际危险相匹配。

所有预备和响应计划均宜以人为本。组织人力资源的管理方式将影响到破坏性事故管理是否成功。

a) 宜设计一个能够在危机发生后迅速通知所有人员的系统。这个系统可使用简单的树形电话网络，或者使用精心制作的外部供应商的电话节目网站。宜保存所有人员的有效和准确的联系信息。宜考虑与本组织的差旅管理部门联系，帮助定位出差的工作人员。

b) 在出现人员受伤或死亡的情况下，宜安排通知相关人员的家属。如果可能的话，宜由最高管理者成员亲自进行通知。宜提供适当的培训。

c) 如果出现严重伤亡事故，组织宜执行家庭代表计划。进行通知的人员和家庭代表不能是同一个人。家庭代表宜作为伤亡人员家庭与组织之间的主要联系人。家庭代表必须经过全面培训。

d) 宜根据需要安排危机咨询。在很多情况下，危机咨询超出了组织的工作人员援助计划（如有）的能力和经验范围。在发生危机情况之前，宜确定其他可靠的咨询来源。

e) 危机可能对组织、其工作人员及其家属，以及其他利益相关方产生影响深远的经济负担；这些经济负担宜被视为准备和响应计划的重要组成部分。经济负担可能包括为受害者的家庭提供经济支持。另外，还可能出现税务问题，这些问题宜预先考虑和澄清。

f) 危机期间宜保持工资管理体系的正常运转。

提前制定后勤决策将影响能否成功执行良好的准备与响应计划。后勤决策包括下列因素。

a) 宜提前确定一个第一危机管理中心。这是危机管理团队和应急响应工作组用于指挥和监督各项危机管理活动的初始场地。此场地宜配备不间断电源、必要的计算机、通信设备、暖通空调系统以及其他保障系统。除此之外，危机管理中心还宜配备紧急备用电源。

b) 如果不能提供专用场地，宜保证为管理团队提供指定场地用于指挥和监督危机管理活动。宜执行出入管理措施，保证所有管理团队的成员可随时出入。

c) 如果第一危机管理中心受到危机事件影响，还宜确定第二危机管理中心。

d) 组织宜考虑成立虚拟指挥中心，实现分布式存取信息，以及联系分散或远距离的利益相关方。

危机管理团队启动之后，宜开始评价损失情况。可由危机管理团队亲自进行损失评价，也可由指定的损失评价小组进行。宜指定专人负责记录事故所有情况下及响应行动(包括财务支出)。

a) 对于涉及公司财产实际损失的情况，危机管理团队或其指定的损失评价小组宜亲自到场进行评价。在获得公共安全管理部门的批准之后，评价团队可进入现场，然后对损坏程度和设施可能无法使用的持续时间进行初步评价。

b) 某些中断类型不会对公司的工作场所或设施造成直接的实际损失。这些危机类型可能包括业务危机、人员危机、信息技术危机和社会危机。对于这些危机，评价小组将随着中断性事件的发展逐步评价各种损失或影响。

在适当的情况下，宜检查现有投资和保险方针，并宜确定和获得额外的资金和保险金额。

a) 宜提前制定方针参数，包括保险提供商预先批准的相关响应的所有供应商。在切实可行的情况下，宜在规划过程中确定保证连续运作的资金总额。

b) 宜将所有现金存放在一个容易进入的地点，确保在危机期间可以动用这些现金；在周末和下班时间，宜可以动用部分现金和存款。

c) 在响应和恢复阶段，宜记录与中断性事件和危机有关所有开支。

d) 在响应阶段，尤其是在广泛存在危机的情况下，宜尽早联系保险提供商，此类资源的竞争可能非常激烈。宜及时向危机管理团队提供所有保险单和联系人信息，并在适当时候进行异地备份或存储。

中断性事件或危机期间的运输问题将是一大挑战。如果可行，宜提前安排各种物资。运输紧张的领域包括但不限于：

a) 人员撤离(包括从被破坏的工作场所或从另一个地区或国家的附属设施中撤离)；

b) 运输至备用工作场所；

c) 工作场所或备用场所的供应物资；

d) 运输到工作场所的重要资料；

e) 运输急需的工作人员。

B.8.7.5 事故连续性与恢复计划

组织宜根据管理部门批准的恢复目标制定文件化程序，详细说明组织将如何管理中断性事件，如何恢复或维持其活动处于预先设定的水平。

a) 宜根据具体情况制定供应链、主要供应商或服务提供商协议，且将相关的联系人信息保存作为准备计划、响应计划、连续性和恢复计划的一部分。如果需要联系不熟悉这一流程的人员，联系人信息可包括电话号码、联系人姓名、账号、密码(适当保护)及其他信息。

b) 为了避免供应链的中断，可适当地请求和评审供应链合作伙伴和主要供应商的准备、响应、连续性和恢复计划，以便评估他们在重大危机情况下继续提供必要的供应品和服务的能力。至少宜在危机之前讨论供应链、供应商或服务提供商的作用及服务水平协议。

c) 组织宜有备用工作场所用于重新开始和恢复业务。如果没有其他可用和/或适用的公司设施，可使用通过适当供应商安排的备用工作场地。关于备用工作场所的识别和可用性规划，宜在准备和响应计划过程中尽早进行。备用工作场所应提供将业务恢复到危险程度、后果和影响分析的规定水平所需的足够资源。

d) 异地存储数据和资产，这是实现快速的危机响应及重新开始/恢复业务的一项重要减缓方针。异地存储位置宜与主要设施保持足够远的距离，确保基本上不会受到同一事件的相同影响。需要考虑的异地存储项目包括对于业务运作至关重要和宝贵的资料（文件和其他媒体资料）。宜将存储程序列入计划中，以确保异地存储的所有重要项目能够及时交付到危机管理中心或备用工作场所。

e) 在供应链中断期间，可与其他组织共享或借用的互助协议识别资源，以及与其他组织共享的相互支持。这些协议宜是合法、完整、合适的文件，各方都清楚地理解，并代表了可靠的资源和合作承诺。

f) 通过战略联盟寻找合作伙伴，与其他组织建立相互合作关系，共同生产和供应产品与服务及分担风险。

g) 在了解损失程度之后，宜优先考虑流程恢复的需求，同时宜制定和记录一份恢复计划。宜优先考虑供应链流程的主要临界点和其他因素，包括供应链义务的关系、其他程序、关键时间表，以及在危险程度、后果和影响分析中所确定的法规要求。关于流程优先次序的决策宜进行记录和存档，包括决策的日期、时间和正当理由。

h) 如果优先考虑恢复供应链流程，可按照优先次序计划表开始流程恢复工作。根据危机的具体情况，可选择在当前工作场所或备用工作场所完成这些流程的恢复工作。在流程恢复之后，宜保存各种文件。

i) 在恢复关键流程之后，也可解决剩余流程的恢复工作。在可行的情况下，宜提前全面记录关于这些流程的优先次序的决策，以及记录实际恢复的时间。

j) 组织宜设法使自己"恢复正常"。如果不可能回到危机前的"正常状态"，宜确定一个"新常态"。这个"新常态"可以理解为，虽然工作场所可能发生变化和改组，但是组织将逐步恢复正常生产工作。宜仔细记录这一过程的每个步骤和所有决策。

k) 通常，此时可正式宣布"度过"危机。宜记录这一重要决策。为了增强工作人员和客户的信心，可召开新闻发布会和通知大众媒体。

B.9 检查和纠正措施

B.9.1 监视

通过分析监视收集的数据，可识别各种模式和获取信息。从这些信息中获取的知识可用于落实纠正和预防措施。宜制定用于衡量韧性管理方针是否成功的衡量标准。

关键特性是组织需要考虑用于确定自身如何管理重大风险，实现目标和目的，以及改善安全、准备、响应、连续性和恢复工作。

如果必须保证结果的有效性，宜根据可追溯至国际或国家标准的测量标准，按照规定的时间间隔，或在使用前对测量设备进行校准或检查。若无此类标准，则需记录校准依据。

B.9.2 合规性与系统性能评估

B.9.2.1 合规性评估

组织宜能够证明自身已经过评价并符合相关法律要求，包括适用的许可证或许可文件。

组织宜能够证明自身经过评价符合其认可的其他要求。

B.9.2.2 演练与测试

测试方案宜利用风险评价识别的事件进行设计。

通过测试可让应急响应团队和工作人员有效履行其职责、明确自己的任务，以及发现韧性管理体系需要纠正的不足之处。参与测试适合于确保韧性管理方针的可靠性和权威性。

测试的第一步宜为设立目标与预期值。主要目标是确定是否可以改进某个中断响应过程的工程及如何改进。其他目标示例包括：

a) 能力测试(如呼入和呼出电话系统性能)；

b) 减少完成整个过程所需的时间(如通过反复练习缩短响应时间)；

c) 将普通员工群体的意识和知识纳入韧性管理体系。

从以前的测试和实际经历事故吸取的经验教训，均宜综合到韧性管理方针循环测试当中。

宜分配韧性管理方针的测试责任。大型组织可考虑成立一个测试小组。在适当的情况下，可利用外部资源(咨询组织、地方应急组织等)的专业知识。

宜制定测试计划及其测试内容的测试进度和时间安排。

测试范围宜设计成随着时间的推移而发展。测试初期宜相对比较简单，然后随着测试过程的发展变得越来越复杂。早期测试可包括检验表、简单演练以及韧性管理方针的细小单元。随着测试进度的发展，测试应变得越来越复杂，直到全部激活整个韧性管理方针，包括公共安全人员和紧急响应人员的外部参与。

测试参与人员可扮演几种不同的角色。所有参与者宜了解自己在演练中的角色，而演练宜包括所有参与者。组织内部团体和公共部门团体均可参加演练。在演练过程中，参与者可相互合作、讨论问题和经验教训。

宜在完成演练和测试之后进行关键性评价。评价内容宜包括：评估测试目的和目标的实现程度、参与效率，以及韧性管理体系本身是否能够在真正危机中发挥预期的功能。宜根据测试结果对未来测试和韧性管理体系本身进行必要的修改。

宜根据需要对测试和演练的设计进行评估和修改。考虑到韧性管理体系的变更，人员变动，实际事故和以前演练结果，宜进行动态演练和测试。

宜记录演练和测试结果。

B.9.3 不合格、纠正措施和预防措施

根据不合格的性质，在制定处理这些要求的程序期间，各个组织可能采用最少的正式规划，或者可能采用一项更为复杂的长期活动来完成制定工作。所有文件宜适用于纠正措施水平。

B.9.4 记录管理

管理体系记录可包括：

a) 合规性记录；

b) 培训记录；

c) 过程监视记录；

d) 检查、保持及校准记录；

e) 有关承包商和供应商的记录；

f) 事故报告；

g) 事故与应急准备测试记录；
h) 审核结果；
i) 管理评审结果；
j) 外部沟通决策；
k) 可适用法律要求的记录；
l) 重大风险的记录；
m) 韧性管理方针会议的记录；
n) 安全、准备、响应、连续性和恢复性能信息；
o) 法律合规性记录；
p) 利益相关方及其他相关方的通知。

宜对机密资料进行妥善处理。

组织宜确保文件的完整性，包括防止文件被篡改、安全备份、只有授权人员才能使用、防止损坏、磨损或丢失。

组织宜与内部法律部门进行适当协商，确定文件应保留的适当时间，并对此建立、执行和维持有效的程序。

注：记录并不是证明本文件合格要求的唯一证据来源。

B.9.5 内部审核

韧性管理方针的内部审核可由本组织内部工作人员或本组织选择代表其工作的外部人员执行。但不论在哪种情况下，负责审核的人员宜有能力完成审核工作，并能够做到公正客观。对于小型组织，审核人员对将要进行的审核活动不承担任何责任，由此证明审核人员的独立性。

注：如果一个组织希望将韧性管理方针审核与安全性或环境审核相结合，宜明确规定各审核目的和范围。

B.10 管理评审

虽然不需要立刻对韧性管理方针的所有要素进行评审，但管理评审仍宜涵盖韧性管理方针的整个范围，并且整个评审程序可能会需要一段时间。

宜定期进行韧性管理方针评审和评估。宜按照预定计划进行评审，并在必要时宜保留评审文件。下列因素可引发评审，并宜在安排评审之后再次检查。

——风险评价：组织每次完成风险评估后都宜对韧性管理方针进行评审。风险评估结果可用于确定韧性管理方针是否依然足以应对组织面临的各项风险。

——部门/行业趋势：主要部门/行业行动宜启动韧性管理方针评审。可将部门/行业及业务/运营连续性规划技术的总体趋势作为参考。

——法规要求：新的法规要求可能需要进行韧性管理方针评审。

——事故经验：宜在中断性事件之后进行韧性管理方针评审。

——测试与演练结果：根据测试与演练结果，宜在必要时对韧性管理方针进行修改。

持续改进和韧性管理方针保持宜反映出可以影响韧性管理体系的组织风险、活动、功能和运作的变化。以下是可能影响韧性管理方针的程序、系统或流程示例：

a) 方针变化；
b) 危险与威胁变化；
c) 组织及其业务流程变化；
d) 供应链的流程、节点和职责变化；
e) 风险评估的假设条件变化；

f) 人员变化(员工和承包商)；
g) 供应商和供应链变化；
h) 工艺和技术变化；
i) 系统和应用软件变化；
j) 从测试吸取的重要教训；
k) 在危机期间实际执行韧性管理方针过程中发现的问题；
l) 外部环境变化(所在区域的新企业、新道路或现有交通模式变化等)；
m) 方案评审与鉴定期间及风险评估期间记录的其他项目。

附 录 C
（资料性）
使用限制

通过系统化方法采用和执行一套韧性管理方法，有助于为所有利益相关方和各相关方取得最理想的结果。但是仅仅采用本文件无法保证能够获得最理想的韧性结果。为了取得最理想的结果，在将韧性管理方针纳入管理体系时，宜在适当、经济上可行的情况下纳入可用的最佳做法、方法和技术。并宜充分考虑这些做法、方法和技术的成本效益。

对于超出组织方针约定范围的韧性性能，本文件不做绝对要求：

a） 遵守适用法律要求及其他组织同意遵守的要求；

b） 支持重大风险预防并将其最小化；

c） 促进持续改进。

本文件正文仅包含一些通用准则，可能作为客观审核的对象。韧性管理方法指南均列明于本文件的其他附录。

本文件和其他标准一样，不是用来制造非关税贸易壁垒，也不增加或改变一个组织的法律责任。实际上，遵守标准要求并未表示免除其法律责任。按照组织的要求，可通过外部或内部审核工序检验其韧性管理方针是否符合本文件要求。检验时可由合格的第一方、第二方或第三方组织执行。检验无需第三方认证。认证仅适用于采用本文件（韧性方针）的管理体系标准。

本文件并未包括质量、职业健康与安全、金融风险管理及其他管理方针的具体要求。

韧性管理方针的细节层次和复杂度、文件范围以及投入资源受到很多因素的影响，如：系统范围、组织规模、组织活动性质、产品、服务和供应链。

本文件规定了安全、准备、危机、应急、连续性、事故和恢复管理计划的通用准则。本文件采用的术语主要强调概念的通用性，但是也承认不同专业使用的术语存在细微差别。为了与 ISO 31000:2009 保持一致，风险评价流程分为风险识别、风险分析和风险评估（其中包括危险、威胁、风险、脆弱性、危险程度、后果和影响分析）。

附 录 D
（资料性）
术语惯例

表 C.1 的术语惯例符合 ISO/IEC 导则 第 2 部分(2004)附录 H“条款表述所用的助动词”的要求。

表 D.1 条款表述所用的助动词

助动词	用法(ISO/IEC 导则 第 2 部分:国际标准结构及编写规则)
应	文件的可审核要求——“用来表示符合标准需要满足的严格要求,并且不允许出现任何偏差。”
宜	建议——“用于表示在几种可能性中推荐特别适用的一种,不提及也不排除其他可能性;或表示某个行动步骤是首选的,但未必是所要求的;或(以否定形式)表示不赞成但也不禁止某种可能性或行动步骤。”
可以,允许	允许——“用于表示在标准的界限内允许的行动步骤。”
能,可能	能、可能——“用于陈述由于材料、生理或某种原因导致的可能性和能力。”

除非另有说明,上表列出的助动词不宜被解释为详尽无遗,也不宜将列表的顺序视为规定其顺序或优先级,除非表中有明确规定。本文件的通用性允许某一组织添加补充项,根据其特定的操作条件和情况制定顺序或优先顺序。

参 考 文 献

[1] GB/T 23694—2013 风险管理 术语

[2] ISO 9000:2005 Quality management systems—Fundamentals and vocabulary

[3] ISO 9001:2000 Quality management systems—Requirements

[4] ISO 14001:2004 Environmental management systems—Requirements with guidance for use

[5] ISO 19011:2002 ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing

[6] ISO 31000:2009 Risk management—Principles and guidelines

[7] ISO Guide 73:2002 Risk management—Vocabulary—Guidelines for use in standards

[8] ISO Guide 73:2009 Risk management—Vocabulary

[9] ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements

[10] ISO/IEC TR 18044:2004 Information technology—Security techniques—Information security incident management

[11] ISO/PAS 22399:2007 Societal security—Guideline for incident preparedness and operational continuity management

[12] ANSI/ASIS.SPC.1:2009 Organizational Resilience: Security, Preparedness and Continuity Management Systems—Requirements with Guidance for Use

中华人民共和国
国家标准
供应链安全管理体系 供应链韧性的开发
要求及使用指南
GB/T 43632—2024/ISO 28002:2011
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.net.cn
服务热线:400-168-0010
2024年3月第一版
*
书号:155066·1-75131

GB/T 43632-2024