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、孔肖菡、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。

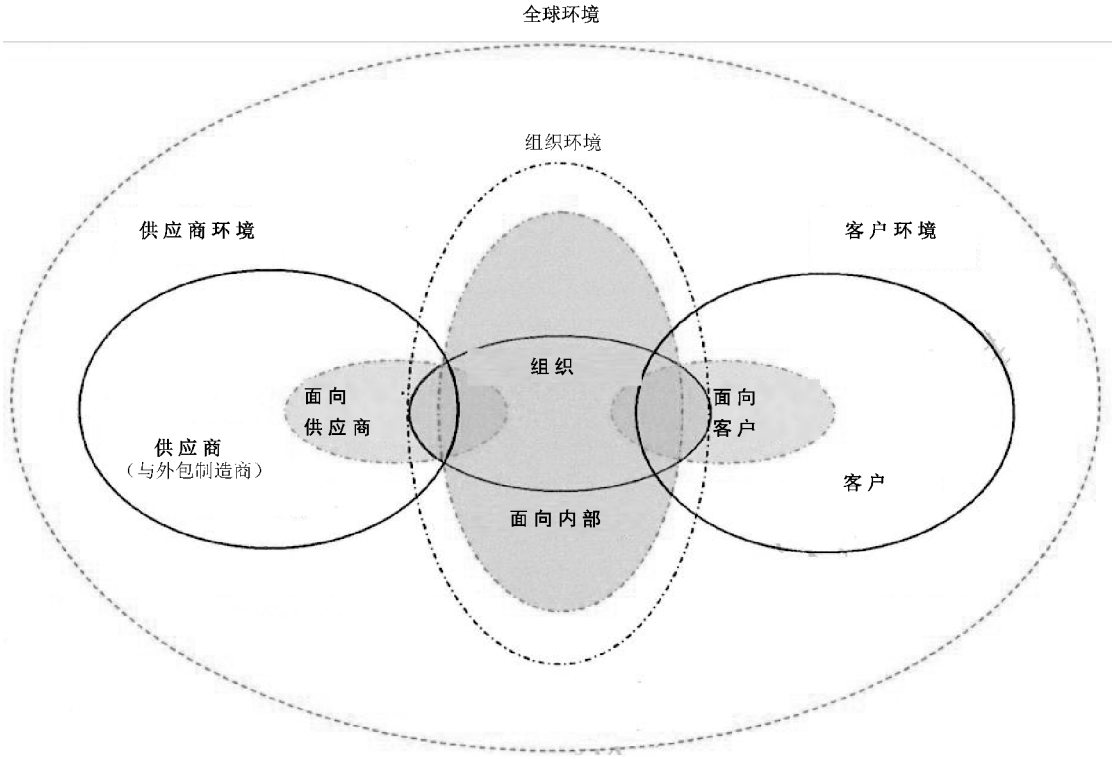

图 1　供应链中的韧性管理方针[资料来源:国际供应链协会(SCC)2007 年]

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。

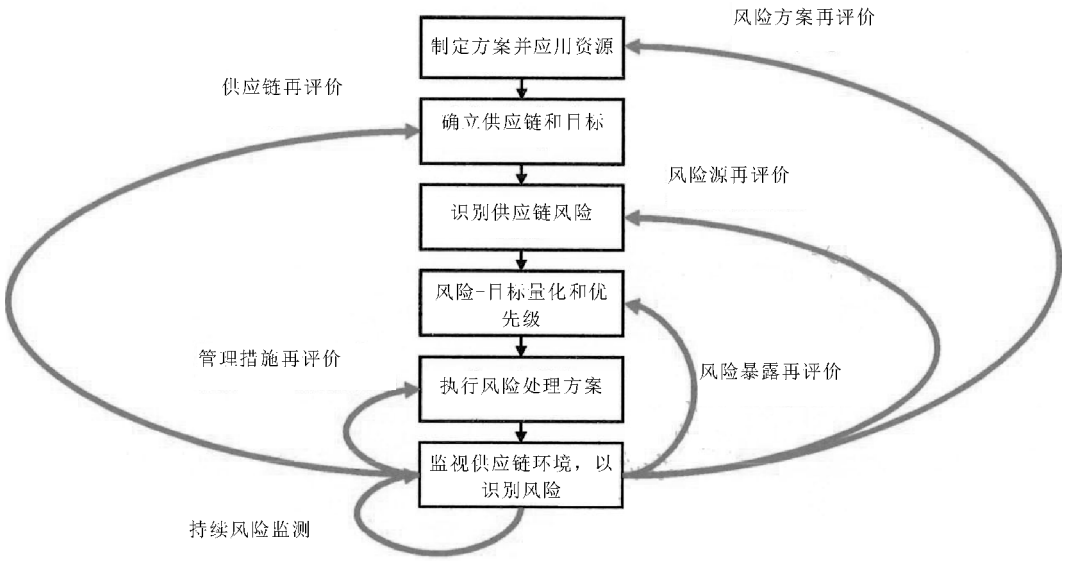

图 2　供应链韧性管理过程方法

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。

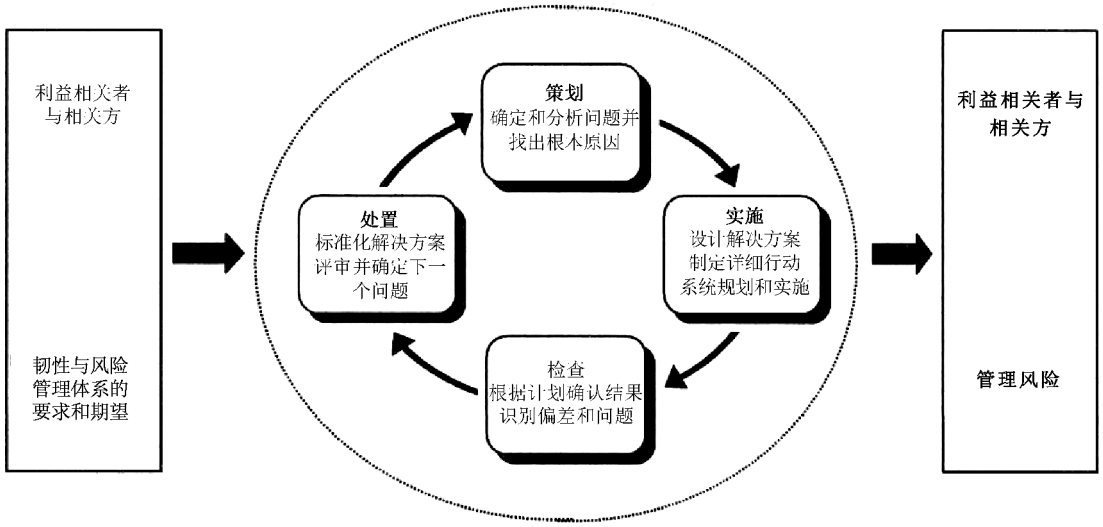

图3　包含韧性方针的管理体系流程图

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。