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/T1.1—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（“(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（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（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、（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（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（防(如可行)中断性（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、（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。

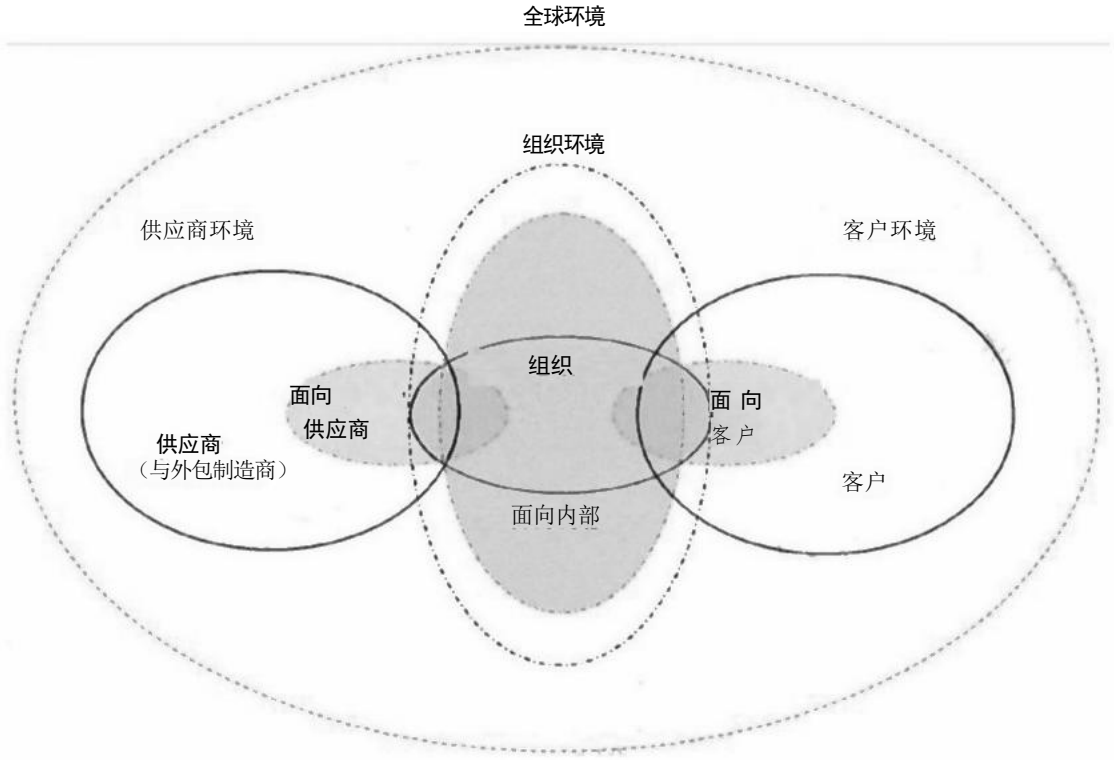

图 1　供应链中的韧性管理方针[资料来源：国际供应链协会（SCC)2007 年]

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。

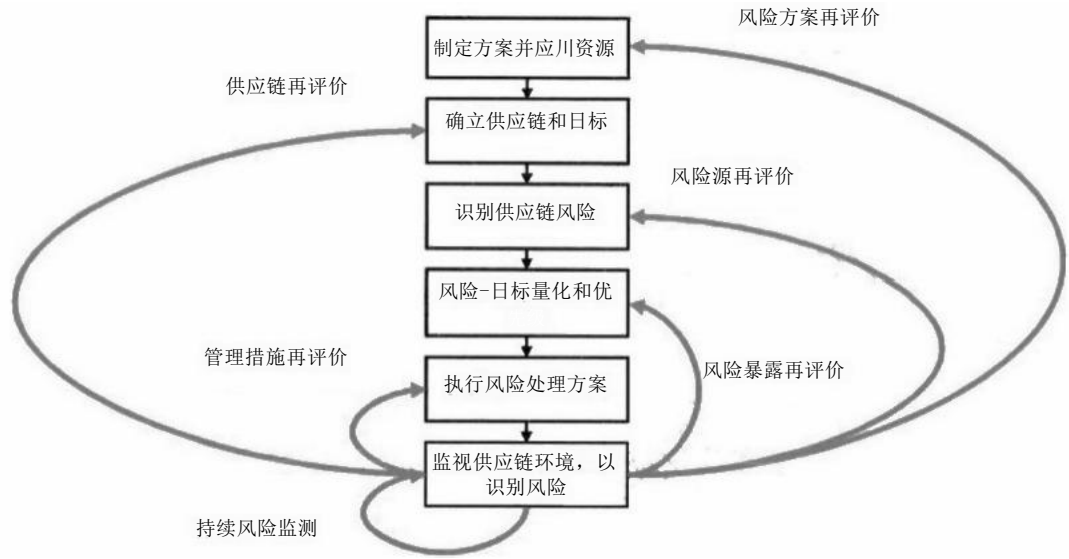

图 2　供应链韧性管理过程方法

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。

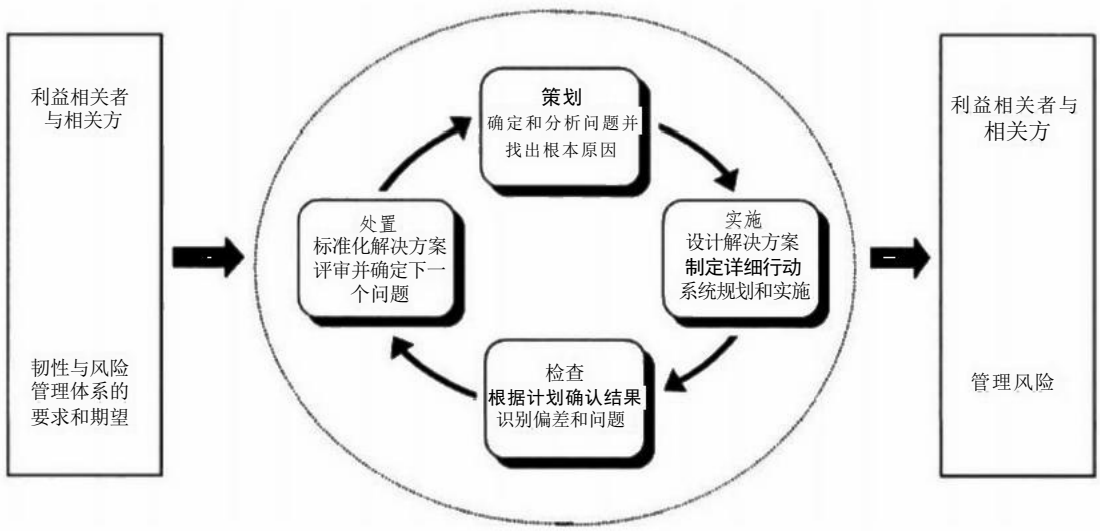

图 3　包含韧性方针的管理体系流程图

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 readines

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/T23694—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/T23694—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：风险而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/T23694—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。

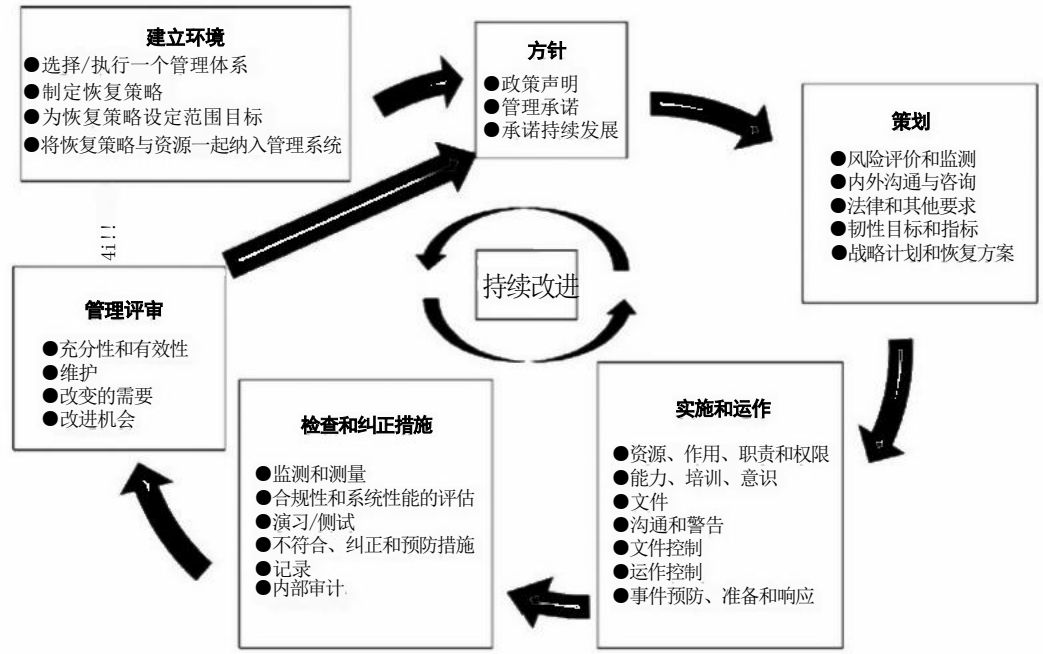

图4　包含韧性方针的管理体系流程图

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：