ICS 03.100.01
CCS A 90

中华人民共和国国家标准

GB/T 42187—2022/ISO 22316:2017

安全与韧性　组织韧性　原则和属性

Security and resilience—Organizational resilience—Principles and attributes

（ISO 22316:2017，IDT）

2022-12-30 发布　　2022-12-30 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。

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。

本文件等同采用ISO 22316:2017《安全与韧性　组织韧性　原则和属性》。

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、烟台嘉量信息服务有限公司、苏州苏大教育服务投资发展(集团)有限公司、北京建筑大学、广东省特种设备检测研究院惠州检测院、北京科技大学、清华大学、山东日辉电缆集团有限公司、北京邮电大学、北京市科学技术研究院、建研防火科技有限公司、国网山东省电力公司、山东大学、浙江圣雪休闲用品有限公司、和也健康科技有限公司、嘉兴市特种设备检验检测院、中国计量大学。

本文件主要起草人:王皖、刘光富、秦挺鑫、许磊、张宏、欧阳小平、吕祥锋、周倩、张超、黄弘、钟茂华、刘锋、胡燕祝、王英剑、徐凤娇、屈莹、王亚飞、杨倚天、孙世军、栾晓嵘、高阳、潘金平、朱伟、王建峰、尹爱辉、朱晓辉、方志财、廖钟财、马德东、王学亮、刘大伟。

引　言

组织韧性是组织承受和适应不断变化的环境，以实现目标并且获得生存和蓬勃发展的能力。韧性强的组织可对内外部环境突变或渐变带来的威胁和机遇作出预测与响应。增强韧性可作为组织战略目标，是良好业务实践和有效风险管理的结果。

组织韧性受战略和执行层面各因素特定的相互作用和组合的影响。组织韧性只有相对的强和弱，不存在绝对的衡量尺度或明确的目标。

增强组织韧性有助于：

——提升预测和处理风险及脆弱性的能力；

——促进管理规程的协调性和整体性，提高凝聚力和绩效；

——加深对支撑战略性目标的相关方及其相关性的理解。

没有单一的方法能够增强组织韧性。目前已存在相关管理规程，但是单靠这些规程不足以保证组织韧性。组织韧性是属性及活动相互作用的结果，也有来自其他科技专业领域的助力。这些会受到不确定因素的处理方式、决策制定和发布及合作方式的影响。

本文件建立了组织韧性的原则，明确了可增强组织韧性的属性及活动。

本文件包括：

——为增强组织韧性奠定基础的原则；

——描述采纳上述原则组织的特征属性；

——指导应用、评估及增强上述属性的活动。

安全与韧性　组织韧性　原则和属性

1　范围

本文件为各种规模和类型的组织增强韧性提供了指导，不针对特定的行业或部门。

本文件适用于组织的全生命周期。本文件不提倡所有组织使用统一的韧性增强方法，而是根据组织的需求定制具体的目标和方案。

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 22300　安全与韧性　术语（Security and resilience—Vocabulary）

3　术语和定义

ISO 22300 界定的以及下列术语和定义适用于本文件。

3.1

管理　management

指挥和控制组织的协调活动。

3.2

相关方　interested party

可影响决策或活动、受其影响、或自认为受其影响的个人或组织。

注：可以是与组织的任何决策或活动有利益关系的个人或团体。

3.3

组织文化　organizational culture

有助于形成组织独特社会和心理环境的共同的信仰、价值观、态度和行为。

3.4

组织韧性　organizational resilience

组织承受和适应环境变化的能力。

3.5

价值观　values

组织所坚持的信念和所遵循的准则。

4　原则

4.1　总则

原则提供了增强组织韧性需要制定、实施和评估的框架和战略基础。

组织韧性：

——当组织行为与其共同愿景、目标一致时，将会得到加强；
——依赖于对组织环境的最新理解；
——依赖于承受、适应和有效应对变化的能力；
——依赖于良好的治理和管理；
——由各种技能、领导力、知识和经验支撑；
——通过协调管理规程和科技专业领域的成果而得到加强；
——依赖于对风险的有效管理。

4.2 协调方法

组织宜制定一种协调办法，以提供：
——授权以确保其领导者和最高管理层致力于增强组织韧性；
——充足的资源以增强组织韧性；
——适当的治理架构以实现组织韧性活动的有效协调；
——韧性活动投入机制，并确保其适合组织的内外部环境；
——支持组织韧性活动有效实施的体系；
——安排以评估和增强支撑组织需求的韧性；
——有效的沟通以增强相互理解和决策制定。

5 组织韧性的属性

5.1 总则

采用了韧性原则的组织将通过活动显示出韧性的共同属性，这些活动指导属性的应用、评估和强化。这些属性包括5.2～5.10中描述的内容。

5.2 共同愿景和明确目标

表述清晰并被充分理解的目标、愿景和价值观有助于组织各级决策的制定，从而增强组织韧性。
组织宜优先考虑并提供资源以支持下列活动：
——向所有相关方阐明其愿景、目标和核心价值观，为决策提供战略方向、凝聚力和明确度；
——确保个人目标一致于并致力于组织的目标、愿景和价值观；
——定期监测和评审组织战略的适宜性及其与目标、愿景、核心价值观的一致性；
——认识到反思的重要性，如有必要，校正组织目标、愿景和核心价值观以应对内外部环境变化；
——寻求和提倡创新理念，以实现和发展战略目标。

5.3 理解和影响环境

全面理解组织内外部环境，有助于组织就韧性优先级作出更有效的战略决策。
组织宜显示并加强以下方面：
——超越当前活动、战略和组织边界的思考能力；
——理解、协调并加强与相关方的关系，以支持组织目标和愿景的实现。
组织宜优先考虑并提供资源给下列活动：
——监测和评估组织的环境，包括在变化中的相互依存性、政治环境、监管环境和竞争对手活动；
——与相关方保持紧密关系，并促进各层面的合作；
——和与组织有共同目标和愿景的相关方合作。

5.4 有效授权的领导力

培养和鼓励他人在各种条件和环境下，包括不确定和中断时期，发挥领导力以增强组织韧性。

组织宜显示并加强以下领导力：

——在组织中鼓励支持韧性的文化；

——能够适应不断变化的环境；

——利用组织内多样化的技能、知识和行为来实现组织目标。

组织宜优先考虑并提供资源给下列活动：

——培养值得信任和尊敬、行事正直、并持续致力于组织韧性的领导；

——分配角色和职责以增强组织韧性；

——鼓励总结和分享经验教训，促进将其用于良好的实践之中；

——授予组织各层级维持和增强组织韧性的决策权。

5.5 支持组织韧性的文化

支持组织韧性的文化显示了共同信念和价值观、积极态度和行为的存在及其承诺。

组织宜优先考虑并提供资源给下列活动：

——确定组织内能界定组织文化的信念、价值观和行为；

——明确增强组织韧性的核心价值观和行为，并建立可用于评估个人绩效的准则；

——鼓励各级人员参与推广组织的价值观；

——培养创造力和创新力以增强组织韧性；

——授权组织成员对威胁和机遇进行识别和沟通，并采取有利于组织的行为；

——监督和审查组织文化，以发现可能影响组织韧性的任何变化。

5.6 共享信息和知识

适时广泛分享和应用知识会增强组织韧性。鼓励经验分享和互相学习。

组织宜显示并加强以下方面：

——注重信息、知识和学习；

——从所有可用的资源中汲取经验（利用其自身所有或从其他组织获得的资源）。

组织宜确保知识和信息：

——可获得、可被理解并足以支持组织的目标；

——有效的分享，以进行决策；

——是组织的关键资源；

——通过既定的体系和过程创建、保留和应用；

——及时与所有相关方共享；

——应用于组织学习。

5.7 资源的可获得性

组织宜开发和分配资源，如人员、场地、技术、资金和信息，以处理脆弱点，提供适应条件变化的能力。

组织宜优先考虑并提供资源给下列活动：

——在提供资源、容量、多样化、备份和冗余方面作出适当决策，以避免单点故障，并对事件和变化作出响应，使核心服务保持在可接受的、预先确定的水平；

——选择和培养具有多种技能、知识和行为的员工，从而提升组织应对和适应变化的能力；

——培养识别和灵活应对变化的能力，包括改造和重新部署性能、安排、结构、活动和行为以调整至新状态；

——定期评审资源的适宜性、可获得性和配置情况，同时考虑到组织及其环境中任何变化的影响。

5.8 管理规程的开发与协调

管理规程的设计、发展和协调及其与组织战略目标的一致性是增强组织韧性的基础。

注：附录 A 提供了管理规程的样本清单。

组织宜进行并加强以下方面：

——协调管理规程，使其单独或共同为组织目标的实现和价值观保护作出贡献 ；

——将组织管理不确定性对其目标的影响贯穿在整个管理规程中。

组织宜优先考虑并提供资源给下列活动：

——识别和设计有助于组织韧性的管理规程；

——定期评估每个管理规程对于组织整体韧性的作用，并在发现薄弱环节时予以解决；

——建立管理规程的灵活性，使组织能够承受和适应变化；

——加强组织管理规程之间的沟通、协调和合作，从而形成一套连贯的方法。

5.9 支持持续改进

当组织根据预先确定的准则持续监测其绩效以从经验中学习和改进并利用机会时，组织韧性将得到增强。组织建立并鼓励一种所有员工持续改进的文化。

组织宜进行并加强以下方面：

——持续改进文化，确保组织目标、战略和程序可以保持相关性和适当性，以支持组织不断变化的需求；

——致力于验证并持续改进组织韧性的活动和能力。

组织宜优先考虑并提供资源给下列活动：

——实施绩效监测和评估机制，以支持持续改进；

——确保绩效管理准则对影响组织目标的变化作出响应。

5.10 预测和管理变化的能力

当组织有能力对变化开展预测、计划和响应时，组织韧性就会增强。

组织宜进行并加强以下方面：

——在不断变化的情况下始终履行其职责并相应调整其运营的能力；

——承受和适应突发和非预期事件影响的能力；

——做好准备以应对变化或必要时影响变化。

组织宜优先考虑并提供资源给下列活动：

——注意可能影响变化的情况；

——在不影响产品和服务的情况下，需要时进行自我调整；

——致力于保护、执行和适应，但有能力在不损害愿景和核心价值观的前提下转移工作重点；

——确保管理规程在应对变化时足够健全和有效。

6 评估影响韧性的因素

6.1 总则

针对组织韧性的战略和目标如何继续满足组织需要或何处有改进机会，评估活动提供资料和管理

信息。

组织宜：

——建立流程，使其能够持续监测有助于组织韧性的因素，以帮助管理决策；

——针对增强组织韧性的特定属性开展监测活动；

——针对这些属性评估其韧性方法和目标的有效性。

6.2 组织要求

6.2.1 概述

评估过程中使用的绩效措施可根据组织所处的部门、最高管理层确定的准则和组织文化来选择。

大多数组织已经收集了可用于评估其韧性的绩效数据，来源可包括现有的管理信息和内审报告、业务评审流程和项目报告。

最高管理层宜：

——为组织韧性确定适当的目标；

——制定用于监测和评估组织韧性属性状态的测量标准；

——监测和评估组织的整体韧性成熟度和绩效；

——识别需要评估和监测的内容，以及能够产生有效结论和持续评估组织韧性的方法；

——确定可接受评估结果的阈值；

——决定评估和监测安排如何与现有监测过程并行，相互支撑或整合；

——确定如何分析、评估和报告监测结果。

6.2.2 确定差距

组织韧性的初步评估可用于为任何急需的工作提供信息，并与相关方一起强化组织韧性的观念。

组织宜：

——在实施监测过程之前进行评审，应用商定的参数来确定组织韧性；

——确定韧性是否为最高管理层所接受或是否符合组织的要求；

——考虑适当的策略，以解决评估中发现的任何重大差距。

6.3 监测与评估

6.3.1 方法与过程

监测和评估组织韧性有助于识别需要关注的新问题或机会出现的迹象。未能识别这些迹象可能会限制组织在问题产生影响之前解决问题的能力和有效性，并增加缓解措施的成本。

组织宜：

——应用现有的监测方法和过程来评估韧性的属性；

——监测为风险管理而制定的措施的有效性，包括根据既定管理规程管理的举措；

——考虑使用员工和客户调查，以获得组织内部韧性指标；

——了解需要哪些数据来进行韧性评估，并确保有一个评估过程来支持这项工作。

6.3.2 审查

最高管理层宜定期进行审查，以确保组织韧性持续达到预期。审查宜考虑组织环境的变化，包括：

——组织愿景、战略或目标的变化；

——重大结构或商业模式变化，包括合并、收购和撤资；

——组织进入的新市场或新领域；

——新引进的产品和服务；
——重大人事变动，包括最高管理层；
——前一次审查后改进措施的有效性；
——组织韧性的有效性反馈；
——需要解决的风险变化。

最高管理层宜：

——将组织韧性评估过程的输出与其他相关评审过程进行比较，如相关内审结果、事件汇报、战略规划、未遂事件和合法合规评审；
——确认监测安排是否适当，并在破坏性影响或错失机会之前，为识别和处理问题提供输入。

6.4 报告

监测组织韧性的输出可包括总结报告、依据与组织最相关的属性作出的给最高管理层的韧性评估。

最高管理层宜：

——利用持续监测报告跟踪评估组织韧性的数据趋势；
——确认当前的信息管理系统提供了组织韧性监测所需的输入数据；
——根据报告过程的输出制定行动计划，以增强组织韧性。

附 录 A
（资料性）
相关管理规程

5.8 中所述的管理规程包括：

——资产管理；
——业务连续性管理；
——危机管理；
——网络安全管理；
——沟通管理；
——应急管理；
——环境管理；
——设施管理；
——财务控制；
——欺诈控制；
——治理；
——健康及安全管理；
——人力资源管理；
——信息安全管理；
——信息、通讯和技术；
——人身安全管理；
——质量管理；
——风险管理；
——供应链管理；
——战略规划。

参 考 文 献

[1] GB/T 23694 风险管理 术语
[2] GB/T 24353 风险管理 原则与实施指南
[3] GB/T 30146 公共安全 业务连续性管理体系 要求
[4] GB/T 38209 公共安全 演练指南
[5] ISO/IEC 38500 Information technology—Governance of IT for the organization