ICS 03.100.01;13.200
CCS A 90

中华人民共和国国家标准

GB/T 45157—2024/ISO 22396:2020

安全与韧性　社区韧性
组织间信息交互指南

Security and resilience—Community resilience—Guidelines for information exchange between organizations

（ISO 22396:2020,IDT）

2024-12-31 发布　　2025-04-01 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 22396:2020《安全与韧性　社区韧性　组织间信息交互指南》。

本文件做了下列最小限度的编辑性改动:

——将3.1的来源由“ISO 22300:2018”改为“ISO 22300:2021”;

——删除了附录B中“私营电力公司”等不符合我国国情的表述;

——参考文献中增加了“ISO/IEC 27000”。

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、应急管理部大数据中心、山东鲁软数字科技有限公司、北京邮电大学、国网上海市电力公司、三门峡社会管理职业学院、中共衢州市衢江区委社会工作部、浙江爱达科技有限公司、中国建筑第二工程局有限公司、山东华特智慧技术有限公司。

本文件主要起草人:徐凤娇、杨继星、秦挺鑫、翟季青、王皖、吴晓涛、黄兴德、胡燕祝、黄帅、屈莹、徐望升、何熊熊、曹福金、李敏、孙世军、王英剑、杨洋、潘爱强、沈晓慧、李平、边路、李佳芮、周永明、苏宪新、宁暑光、张雨璠、岳立峰。

引　言

对于社会中的所有行动者而言，风险的格局已经发生了变化，包括政府机关、企事业单位以及其他组织。组织之间的相互联系和相互依存更加紧密，从而导致了跨领域和叠加风险。

关键社会基础设施或服务逐渐由各类主体参与管理，这对以能力建设为目的的组织间合作和信息交互提出了新的要求。关键社会基础设施和服务的所有权模式的变化意味着政府机关、企事业单位以及其他组织需要参与制定提高应对能力、增加经验和增进知识交流的机制。

虽然属地政府肩负服务和保护公民的责任，提高关键社会职能的安全性的预防措施传统上被视为政府机关和公共部门的核心领域，但解决方案往往来自社会各方。为了提高社会安全并提升韧性，强化和支持预防性保护措施，政府机关、企事业单位以及其他组织的行动者有必要有效和安全地交互信息。

一般来说，协作的目的是识别风险并且发起各种行动，以提高安全性并且降低脆弱性。通过针对可能的责任、威胁以及脆弱性开展信息交互，可以提高组织运作的效力和效率。

在组织之间建立准确的信息共享边界是具有挑战性但必要的。由于协调这些领域需要针对每个不同的行业、地区或国家制定特殊的解决方案，因此协调责任也难以确定。

企业也需要确保其敏感信息不会被泄露，不被用于妨碍竞争或者损害其经营活动和品牌。因此，安全的信息交互是政府机关、企事业单位以及其他组织成功、有效信息交互的必要条件。

参与信息交互的组织可以增加对事件和风险的了解和理解，以强化韧性。有效的信息交互可以为此类组织带来其他效益，其中包括：

——为可能无法获得访问权限的组织提供指导；

——通过其他方式开放限制信息来强化能力；

——创建集中式信息交互以支持共享；

——提高信息分发能力；

——通过关怀和共享，建立组织责任感。

本文件分为三大部分：原则、框架以及流程。原则为本文件的核心内容，框架确定了进行信息交互的必要要素，流程描述了确立和维护该信息交互的程序。图 1 给出了原则、框架和流程之间的关系。

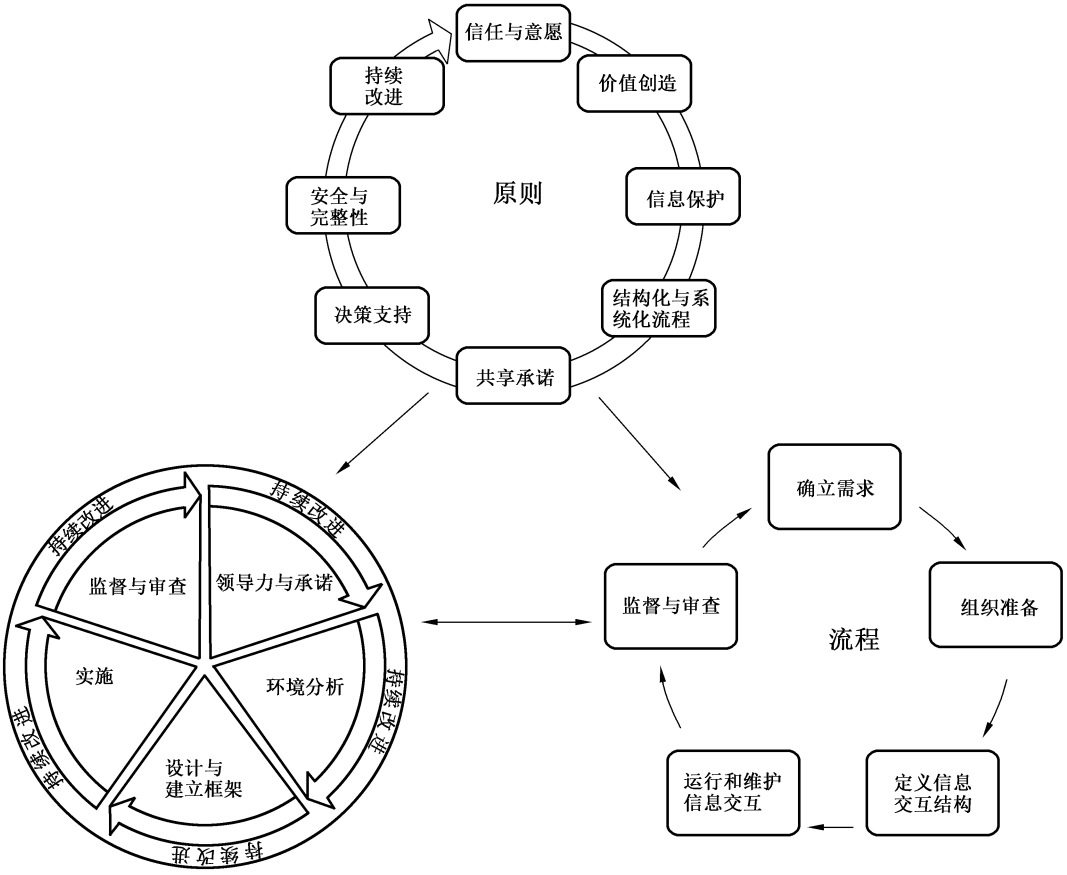

图 1　原则、框架和流程间的关系

安全与韧性　社区韧性
组织间信息交互指南

1　范围

本文件提供了组织间信息交互指导，确定了信息交互的原则、框架以及流程，使参与组织能够从他人的经验错误或成功中学习，并提供相关措施来强化组织应对风险的能力。

本文件适用于对需要建立支持信息交互条件相关指导的私人和公共组织。

本文件不适用于具体技术层面，主要侧重于方法论。

注：法律规范因不同法域而异。文件使用者需自行负责确定相关法律规范与本文件之间的适用关系。

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）

注：GB/T 44483—2024　安全与韧性　术语（ISO 22300:2021，MOD）

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

敏感信息　sensitive information

对组织、国家安全或公共安全可能产生不利影响而不公开披露的信息。

[来源：ISO 22300:2021，3.1.260，有修改]

4　原则

4.1　概述

信息交互的总体目标是在受信任的组织之间共享信息，作为知情决策的一部分，以提高安全性和韧性（示例见附录 B）。组织的特定需求和具备资源不同使每次的信息交互具有独特性，因此在信息交互的初始阶段即宜制定相应的原则来指导信息交互，使其得以有效评估和持续改进。

4.2　指导原则

为有效开展信息交互参与组织宜遵循下列指导原则。

a）　信任与意愿：基于信息交互（包括敏感信息）的信任和意愿。

b）　创造价值：基于互利的基础上，创造和保护组织的价值。

c）　信息保护：信息交互需要对每个参与组织指定的敏感信息达成相互理解。

d）　结构化与系统化流程：各组织在遵循信息政策、流程和惯例、相关立法法律法规以及隐私原则