



中华人民共和国国家标准

GB/T 46409—2025

风险管理 新兴风险管理指南

Risk management—Guidelines for managing an emerging risk

(ISO/TS 31050:2023, Risk management—Guidelines for managing an emerging risk to enhance resilience, MOD)

2025-10-05 发布

2025-10-05 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 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 新兴风险 2

 4.1 新兴风险的本质 2

 4.2 新兴风险的特征 3

 4.3 新兴风险的演变 5

 4.4 新兴风险管理与组织韧性的关系 5

5 原则 6

 5.1 概述 6

 5.2 整合 6

 5.3 结构化和全面性 6

 5.4 定制化 6

 5.5 包容性 6

 5.6 动态性 6

 5.7 最佳可用信息 6

 5.8 人和文化因素 7

 5.9 持续改进 7

6 过程 7

 6.1 GB/T 24353—2022 过程在新兴风险中的应用 7

 6.2 沟通和咨询 7

 6.3 范围、环境、准则 8

 6.4 风险评估 9

 6.5 风险应对 11

 6.6 监督和检查 11

 6.7 记录和报告 12

7 通过新兴风险管理提高组织韧性 12

 7.1 能力发展 12

 7.2 新兴风险和韧性指标 14

8 风险情报循环和新兴风险管理 15

 8.1 概述 15

8.2 将知识应用于新兴风险决策	16
附录 A (资料性) 可能成为新兴风险来源的情境变化示例	17
附录 B (资料性) 新兴风险描述或记录模板的示例	18
附录 C (资料性) 系统性风险	19
附录 D (资料性) 可能影响管理新兴风险的因素示例	20
附录 E (资料性) 管理新兴风险的风险情报循环	22
附录 F (资料性) 韧性指标模板示例表	25
参考文献	27

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。

本文件修改采用 ISO/TS 31050:2023《风险管理 新兴风险管理指南：增强韧性》。

本文件与 ISO/TS 31050:2023 相比做了下述结构调整：

——图 1 对应 ISO/TS 31050 的图 2，图 2 对应 ISO/TS 31050 的图 3，图 3 对应 ISO/TS 31050 的图 4。

本文件与 ISO/TS 31050:2023 的技术差异及其原因如下：

——用 GB/T 24353—2022 替换规范引用 ISO 31000(见第 3 章、5.1、5.2、6.1、6.2、6.3.1、6.4.1、6.5、6.6、6.7、8.2，ISO/TS 31050:2023 的第 3 章、5.1、5.2、6.1、6.2、6.3.1、6.4.1、6.5、6.6、6.7、8.2)；

——用 GB/T 27921 替换规范引用 IEC 31010(见第 3 章、6.4.2、6.4.3、6.5，ISO/TS 31050:2023 的第 3 章、6.4.2、6.4.3、6.5)；

——用 GB/T 42187 替换规范引用 ISO 22316(见第 3 章、4.4，ISO/TS 31050:2023 的第 3 章、4.4)；

——用 GB/T 44483 替换规范引用 ISO 22300(见第 3 章，ISO/TS 31050:2023 的第 3 章)；

——增加了“系统性风险”的术语和定义(见 3.7)，以便于更好地在中文语境中理解本文件的内容；

——增加了“风险情报循环”的术语和定义(见 3.8)，以便于更好地在中文语境中理解本文件的内容；

——删除了图 1，更改了相关表述，避免可在 GB 24353—2022 中查询、无实质性意义的图占用本文件过多篇幅(见 5.1，ISO/TS 31050:2023 的 5.1)。

本文件做了以下编辑性改动：

——为与现有标准协调，将标准名称改为《风险管理 新兴风险管理指南》；

——删除附录 A 中自然灾害(极端天气事件)中使用的美国示例，使用更一般性的示例进行说明；

——删除附录 F 中的提供者“CCPS Center for Chemical Process Safety, AIChE, <https://www.aiche.org/ccps>”，修改为“××专业类协会”，以保障模板示例的一般性。

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。

本文件由全国风险管理标准化技术委员会(SAC/TC 310)提出并归口。

本文件起草单位：三门核电有限公司、中国标准化研究院、中煤能源研究院有限责任公司、佛山市乐华恒业厨卫有限公司、核电运行研究(上海)有限公司、中国石化工程建设有限公司、中国航发南京航空动力有限责任公司、浙江永安工程咨询集团有限公司、国投新疆罗布泊钾盐有限责任公司、中核苏能核电有限公司、中国航空发动机研究院、中共中央党校(国家行政学院)、中国人民大学、中核能源科技有限公司、四川诚至诚烟草投资有限责任公司、河北省烟草公司秦皇岛市公司、江苏核电有限公司、广东坚美铝型材厂(集团)有限公司、城市安全发展科技研究院(深圳)、达信评(北京)风险管理咨询有限公司、杭州宫延楼文化发展有限公司、成都产品质量检验研究院有限责任公司、中科健康产业集团股份有限公司、国家市场监督管理总局认证认可技术研究中心、陕西延长石油集团四川销售有限公司、西北大学、多场低温科技(北京)有限公司。

本文件主要起草人：陆小伟、张冰伟、洪利斌、侯涛、罗建、朱磊、宁秀丽、李群、崔方水、石岭、张斗群、胡春平、王朋格、刘剑、李亚、宋荷靓、程闻、赵思萌、游志斌、张鹏、张爱林、施钟淇、崔文惠、刘鹏飞、张伟、尹健康、石琦、孙友文、唐钧、景一鸣、谢炜、吴强、支凤春、毛瑞华、王飞轮、李金柱、周亚杰、李卫华、古文哲、周玉焕、徐龙辉、程海星、田雨露、何金城。

引 言

新兴风险具有新颖性、数据不足和缺乏决策所需的可验证信息等三大特点,导致相关决策面临挑战。这类风险可能带来重大威胁与机遇,因此宜将新兴风险管理作为组织风险管理的一部分。宜包括与组织外部环境的多个方面相关情况或条件的变化及对其内部环境的影响。

管理新兴风险宜聚焦于知识并依赖于积累可验证的数据和信息,尤其是当这些数据和信息有限或不一致时。通过解释,这些信息形成知识,并为战略、战术和运营决策提供情报。

为此,本文件提供了将 GB/T 24353 应用于管理新兴风险以增强组织韧性的指南。重点关注对组织及其目标可能产生重大后果的新兴风险。

具体指导包括:

- 如何理解新兴风险的本质和特征(见第 4 章);
- 风险管理原则如何适用于新兴风险(见第 5 章);
- 如何将 GB/T 24353 给出的风险管理过程应用于新兴风险(见第 6 章);
- 如何通过管理新兴风险增强韧性(见第 7 章);
- 如何利用风险情报循环来管理新兴风险(见第 8 章)。

详情见附录 A~附录 F。

应用本文件有助于组织获益于:

- 提高意识,降低未能预测新兴风险的可能性;
- 早期识别新兴风险,提高准备和韧性水平;
- 及时向利益相关者传递数据并交换信息;
- 在组织的各个方面协调行动,以应对新兴风险。

风险管理 新兴风险管理指南

1 范围

本文件为组织可能面临新兴风险的管理提供指导,内容包括新兴风险的管理原则、过程,通过新兴风险管理提高组织韧性,风险情报循环等。

本文件适用于各类组织,涵盖组织的任何发展阶段及所有活动领域。其实施可根据不同组织或其具体情境进行定制化调整。

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。

- GB/T 24353—2022 风险管理 指南
- GB/T 27921 风险管理 风险评估技术
- GB/T 42187 安全与韧性 组织韧性 原则和属性
- GB/T 44483 安全与韧性 术语

3 术语和定义

GB/T 24353—2022、GB/T 27921、GB/T 42187、GB/T 44483 界定的以及下列术语和定义适用于本文件。

3.1

韧性属性 resilience attribute
组织吸收和适应环境变化能力的特征。

3.2

知识 knowledge
通过学习吸收信息所获得的结果。
注 1: 知识能通过研究、经验或教育获得。
注 2: 知识包括与某一工作或研究领域相关的信息、事实、原则、理论和实践。
注 3: 知识是个人或集体的。集体知识是通过人们的协作,并释放其隐性及潜意识知识。
[来源:ISO 56000:2020,3.4.1]

3.3

情报 intelligence
通过收集、分析和解读数据、信息及知识(3.2)所获得的结果。
注: 情报有多种类型,例如(但不限于)市场情报、技术情报、竞争情报、知识产权情报或商业情报。
[来源:ISO 56006:2021,3.1]

3.4

组织韧性 organizational resilience
组织在不断变化的情境中吸收、恢复和适应的能力。

[来源:GB/T 44483—2024,3.1.164,有修改]

3.5

突破性创新 breakthrough innovation

具有高度变革性的创新。

注 1: 变革涉及实体或其影响。

注 2: 突破性创新与渐进性创新处于创新连续体的两端。

[来源:ISO 56000:2020,3.1.1.1]

3.6

颠覆性创新 disruptive innovation

最初满足较低需求、逐步取代现有方案的创新。

注 1: 与现有方案相比,颠覆性创新最初形式更简单、性能较低,但通常更具成本效益,所需资源更少且价格更低。

注 2: 当相当比例的用户或客户采用该创新时,即发生颠覆。

注 3: 颠覆性创新能通过吸引新用户及采用新型商业与价值实现模式,创造新市场与价值网络。

[来源:ISO 56000:2020,3.1.1.2]

3.7

系统性风险 systemic risk

可能会导致相关系统大规模失效或对其产生重大影响的不确定性因素。

注 1: 系统性风险具有高度复杂性、影响跨界或跨领域、联动性、非线性等典型特征。

注 2: 实践中,也会使用系统性风险表示某一类风险的属性。

3.8

风险情报循环 risk intelligence cycle

由对多重环境进行扫描的外部循环和包括框架、数据收集与分析、信息解释、情报等步骤的内部循环共同构成的风险情报环路。

4 新兴风险

4.1 新兴风险的本质

新兴风险的本质(可能成为新兴风险来源的情境变化示例见附录 A,新兴风险描述或记录模板的示例见附录 B)可能包括:

- 组织先前未识别或经历过的风险;
- 现有知识不适用时,在新的或不熟悉的情境中出现的已知风险;
- 显著变化的风险;
- 系统性风险(见附录 C);
- 风险的新组合。

即使组织未考虑新兴风险,也不意味着其不会受到影响。在许多情况下,初期往往无法构建相关情景、预估事件发生可能性、预判后果或确定控制措施选项。为更好地理解特定新兴风险的本质,宜参考那些已有更好认知的类似风险本质。

上述风险可能源于组织为实现目标所处环境的变化,包括但不限于:

- 组织关系;
- 获取资本和能力;
- 与社会、地缘政治、环境、经济、技术、法律、感知(相关示例见附录 D)和伦理因素的相互作用或相互依赖关系;
- 业务的内部治理、文化和运营方面。

新兴风险宜在观察组织环境变化之中被识别和描述。新兴风险通常表现为一系列新出现的、既往未被识别的环境条件,或已识别风险特征的显著变化。此类变化可能涉及:

- 社会规范;
- 组织文化;
- 感知;
- 与风险或风险演变方式相关的数据,或根据数据解读的信息。

注:有些风险是在几乎没有预警的情况下出现的。

4.2 新兴风险的特征

4.2.1 概述

有效及高效地管理新兴风险,宜持续获取组织职能、运行环境、经验、数据访问及新兴风险特征方面的知识(如通过应用风险情报循环,见第8章及附录E)。所获取的数据、信息及知识宜适当记录(见6.7及附录B)。

以下因素对新兴风险的新认知尤为重要:

- a) 与预期结果或后果(无论积极或消极)可能存在的偏差及其发生可能性;
- b) 风险的来源和本质;
- c) 其他因素,如风险的发展速度和可探测性。

若组织此前未经历过特定的环境变化,则可能出现相关数据有限或新兴风险特征未完全显现的情况(如系统性风险,见附录C)。在具有波动性、不确定性、复杂性及模糊性的环境中,理解新兴风险背景的特征取决于当前可获取的关于风险本质与来源、数量与时间维度的知识。因此,所获知识可能不足以识别风险特征变化和潜在来源;即便已识别出新兴问题,也可能难以判定其偏离预期的可能性与后果。

由于高度不确定性,数据和信息的解读可能受个体认知偏差影响(见附录D)。

新兴风险的特征宜参考以下要素进行分类。

——知识要素,包括但不限于:

- 组织背景中未知的变化;
- 变化的微弱信号易受到解读和偏见的影响;
- 不足以判定可能性及后果的数据。

——波动性要素,包括但不限于:

- 可能快速或不可预测变化的条件或环境;
- 未知变量变化的影响及后果;
- 数据和信息的不稳定性。

——不确定性要素,包括但不限于:

- 从早期预警信号到新兴风险的演变;
- 新兴风险来源的判定。

——复杂性要素,包括但不限于:

- 系统、部件或流程的高度互联性;
- 组织环境中未知的相互依赖性;
- 新兴风险与其他风险或活动相互作用,可能导致的非线性效应;
- 某些风险的系统性本质(见附录C);
- 潜在决策和后果的高度复杂性。

——模糊性要素,包括但不限于:

- 可作多重解读且受个体认知影响的有限数据;

- 缺乏知识与情报发展的先例；
- 情境变化的因果关系缺乏明确性。

——时间维度要素,包括但不限于:

- 组织环境的变化速度；
- 新兴风险特征的变化速率。

——可控性要素,包括但不限于:

- 组织在内部或外部环境中,无法控制的影响因素。

——行为要素,包括但不限于:

- 环境、人员、系统或流程中突发变化的影响(见附录 D)。

并非所有新兴风险都必然具备上述全部特征,这些特征也非新兴风险独有。但上述分类体现了新兴风险的共性主题,宜在风险管理时加以参考。

4.2.2 知识方面

关于新兴风险的知识宜基于可用数据的数量、质量以及其作为可靠信息的可用性,以支持决策制定。为有效管理新兴风险,宜考虑使用可收集和解读有关外部环境中能力、可能性、变化及趋势数据的系统,同时宜考虑对新兴风险特征及其对组织目标影响的理解,可能仍受限于数据缺失或不足的情况。

宜特别注意的是,在知识缺乏的情况下,对新兴风险的理解可能受个体感知、认知偏差、群体效应、错误信息或误判的影响,从而导致无法可靠评估其发生可能性和后果。此类情形下,新兴风险管理的重点宜转向评估风险的合理性并提升组织的韧性。

随着新兴风险的演变,对这些风险及其特征的认识也在不断发展。

注:初期阶段,组织对特定情境下潜在问题的理解可能极为有限。随着数据与信息的收集和解读,认知逐步深化,从而能够识别新兴风险并研判其潜在后果。

这一过程宜在风险情报循环(见第 8 章及附录 E)中系统化实施,通过将知识转化为战略情报来优化决策。

4.2.3 度量方面

可用数据和信息的质量(如完整性、可靠性、准确性、及时性、相关性)对于获取知识以对新兴风险特征进行度量(包括后果和可能性)至关重要。组织宜建立系统,及时获取微弱信号或早期预警的相关数据,并对数据及新兴风险特征的变化进行分析。这种分析宜包括信息的模糊性,对新兴风险发展认知的局限性,以及组织环境中的趋势和模式,来揭示潜在新兴风险的来源。

4.2.4 时间维度

对新兴风险的特征描述宜包括时间维度,例如获取风险认知和管理所需信息的速度。了解新兴风险的时间特征将影响数据收集和分析、信息解读、知识构建过程以及决策时效性。获取必要信息的时间,可用会影响风险管理的管控选项和所需专业知识的覆盖范围。

新兴风险的关键时间特征指标宜包括:

- a) 条件或情况变化的速度(速率);
- b) 新兴风险的发展速度;
- c) 从环境或条件变化到识别出新兴风险的前置时间;
- d) 获得信息、知识和情报转化为有效信息的时间;
- e) 组织变化和出现微弱信号或早期预警之间的时间间隔;
- f) 从风险识别到事件发生的时间。

4.2.5 易变性方面

新兴风险的特征可能导致不确定或意外的变化和波动,例如:

- 突然认识到情况了解不够充分,组织对潜在的重要数据并不了解;
- 环境、能力和对这些变化的理解发生了意料之外的阶梯式变化;
- 组织环境的快速和不可预测的变化以及未预见的改变。

信息宜不断更新,以增加对这些变化原因的理解。这些特征和知识宜作为对新兴风险有效和高效决策的一部分。

4.3 新兴风险的演变

了解组织背景的各个方面宜被视为有效识别、分析和评价新兴风险的关键(见 4.1)。这些环境方面的任何变化或所有变化都会导致组织背景的改变,并可能对组织目标产生积极或消极的影响。

组织背景任何方面出现的微弱信号和初期变化指标,都是潜在新兴风险的征兆。在此种情况下,组织宜持续监测已识别的变化,并不断收集、分析数据,以评估各要素变化的重要性,并构建相应情景。

密切监测和评估环境变化,并持续增加可用数据(如可能性、变化速率、影响程度和易变性、时间范围和背景等各个方面),将有助于提升对已识别问题和潜在新兴风险的理解。

在新兴风险演变的初期阶段,特别是对新兴风险缺乏认识 and 经验的组织,宜意识到数据可能不可用、有限、不一致、不准确或虚假。因此,将数据转化为可验证的信息用于决策制定,宜着重减少重大不确定性。

尽管持续监测和评估新兴风险特征的变化通常会增加收集数据的质量和数量,但组织宜意识到,并非所有环境变化都能被情景分析识别或覆盖。

4.4 新兴风险管理与组织韧性的关系

组织韧性是指一个组织在不断变化的情境中吸收、恢复和适应的能力。组织韧性使一个组织能够实现其目标,生存并繁荣。组织环境的变化通常是最初的指标,或是识别威胁和机遇、脆弱性及新兴风险源的指标。

应对潜在威胁方面,组织韧性使组织能够做好应对准备,吸收其影响,快速恢复并适应不断变化的环境。把握潜在机遇方面,组织韧性使组织能够从变化中获益,创造内部价值并自信地承担适度的风险(见 GB/T 42187)。

高效和有效的新兴风险管理,宜有助于避免和减轻可能无法利用机会,或对组织的重要目标甚至组织的生存产生不利影响。

因此,组织宜采用和应用韧性与韧性指标的原则(见附录 F),发展增强其生存和繁荣的能力和特征。一个组织预判、准备和应对变化的能力是有效管理新兴风险的核心要求。因此,具备韧性的组织宜具有以下典型能力特征,包括:

- 预见能力:预见能力指通过必要的能力和功能应对任何类型的意外事件,无论是有利或是不利,这也意味着,在竞争对手之前准备好利用外部环境变化带来的潜在机会;
- 抵抗和恢复能力:抵抗和恢复能力指抵抗不利情况并在受到干扰后恢复正常状态的能力,超出维持和恢复组织功能的范围,重点是推进组织流程和能力;
- 适应能力:适应能力指有效制定特定情境下的应对措施,适应破坏性事件,并最终开展变革性行动以利用颠覆性事件的能力。

在发生破坏性事件之前,宜根据组织成功管理类似意外事件的程度来衡量组织的韧性水平。组织韧性宜包括可实现对新兴风险的有效预测和适应的能力。

5 原则

5.1 概述

风险管理的核心和目的是创造和保护价值。为实现目标,GB/T 24353—2022 给出的一系列基本原则,同样适用于新兴风险的管理。

5.2~5.9 针对如何将这些原则应用于新兴风险的管理提供了补充建议。在应用这些原则时,组织宜确保新兴风险:

- 在其出现的阶段不断开展评估,以提高对风险特征及态势的认知和理解;
- 基于多种未来可能情境开展评估。

此外,组织宜认识到信息和数据的局限性、不一致性和可变性,确保威胁和机会得到充分管理。

5.2 整合

除 GB/T 24353—2022 提供的内容外,无补充性指导建议。

5.3 结构化和全面性

组织宜在必要时采用敏捷方法来收集和解读数据,生成信息,并将知识转化为决策者可用的情报(见第 8 章和附录 E)。

组织宜明确考虑是否需要获取数据(包括结构化和非结构化数据),并将其解释为信息以及应用知识,以满足全面风险管理的综合方法的要求。

该方法宜强调持续的识别工作以及对新兴风险的沟通的重要性。

5.4 定制化

组织宜确保其风险管理框架和过程能够根据新兴风险的波动性、不确定性、复杂性和模糊性特征进行定制,并与其使命、目标和战略保持一致。

5.5 包容性

组织宜以适当且及时的方式识别并吸引对新兴风险感兴趣的利益相关者参与,通过学习可应用的利益相关者的经验,提高组织的知识水平。

即使数据质量较差且信息有限,只要信息来源具有足够的可信度和专业性,组织宜认可该信息的可信度。

5.6 动态性

组织宜考虑环境中出现意外和颠覆性变化的可能性,并建立及时预测、发现和应对变化的能力。因此,组织宜保持足够的敏捷性、灵活性和适应性,以适应外部环境中可能发生的合理变化。

组织宜确保其风险管理框架包含能够预测和应对不断变化情况的组成部分,并在风险管理过程中保持足够的灵活性。组织成员宜能够适应并应用不同的工具和技术来应对新兴风险的特征。

5.7 最佳可用信息

鉴于评估新兴风险时缺乏历史和相关的现行信息,组织宜确保持续开展数据收集、验证和数据分析工作,以提取与新兴风险相关的信息,为决策提供最佳信息来源。

第 8 章就如何收集所有可用数据,并生成针对新兴风险决策的有价值情报进行了进一步指导。

5.8 人和文化因素

组织宜认识到,有关新兴风险的事实缺乏可能会颠覆既有认知。基于此原因,新兴风险信息可对人类文化和行为产生重大影响。因此,宜重视内部和外部专家的贡献。

组织宜认识到,随着新兴风险的发展,数据可用性及其向可信信息的转化可能会发生显著变化,早期的认知可能会被证明是错误的,既定观念也可能面临挑战。

5.9 持续改进

组织宜确保新兴风险管理能够为社会和商业带来新的机遇、新的学习和新的体验,包括对以往风险分析结果的批判性审查。组织宜明确将这种新认知作为知识开发、风险管理内外过程优化和实践创新的催化剂。

组织宜确保不断改进以实现对新风险的有效和高效管理。改进宜包括数据收集、信息转化与共享,以及在应用风险管理流程的同时进行知识创造与升级。

有效管理新兴风险宜具备前瞻性,该能力同样适用于市场情报工作、公共和私营部门新产品和服务开发。管理新兴风险对于目标实现和服务交付,并在满足当前需求的同时布局未来至关重要。

6 过程

6.1 GB/T 24353—2022 过程在新兴风险中的应用

组织宜根据 GB/T 24353—2022 第 6 章(见图 4)描述的风险管理过程管理新兴风险,并将活动整合到组织的结构、体系、运营和过程中。新兴风险的相关性宜在组织各层级及职能中予以考虑。

将 GB/T 24353—2022 过程应用于新兴风险时,宜采用具有足够灵活性的结构化方法,以适应新兴风险认知的动态更新。例如,通过风险分析获得的知识可应用于预测环境变化。

新兴风险可能相互影响,也可能影响组织面临的其他风险。通过考虑可能的依赖关系与相互关系,组织宜将风险视为系统性问题,而非孤立或个别问题。一种分析依赖性、关联性和相互联系的方法宜考虑整个系统,而非仅分析单一风险要素。

第 8 章和附录 E 所述的风险情报循环,可为组织及其决策者应用 GB/T 24353—2022 中描述的风险管理过程提供帮助。

6.2 沟通和咨询

除 GB/T 24353—2022 中 6.2 外,以下建议也适用。组织宜确定内部和外部利益相关者并建立沟通渠道,以便在需要采取行动时能够及时沟通。与其他风险一样,利益相关者宜包括应被告知的人、将被征求意见的人及将参与风险管理过程不同环节的人。利益相关者会随着时间推移而变化,不同的利益相关者可能涉及不同的风险管理要素。例如,广泛经验和专业知识可帮助识别新兴风险,而对特定风险的分析可能需要特定领域专家。

与相关利益相关者互动有助于识别新兴风险,使利益相关者能够提供信息以支持决策,并对其实施情况提供反馈。这种互动促进了有关新兴风险的信息和知识可在不同的利益相关者之间(例如专家、监管机构、股东、消费者、媒体、合作伙伴、供应商、公众)共享。通过这种方式,各方能就风险本身及其管理措施的必要性达成共识。

在首次识别出新兴风险时,可能对其影响了解较少,因此不同利益者对其组织重要性的认知可能出现分歧。沟通对于处理可能出现的认知分歧至关重要(例如,受社交媒体的影响或在媒体来源中呈现虚假或误导性信息)。

快速演变的新兴风险可能需要迅速决策,进而突出了加强沟通和征询意见的必要性。宜考虑其他

组织或利益相关者(如合作伙伴、客户、供应商等)是否经历过类似情况,以尝试获取有关数据和信息。

组织宜:

- 建立有效机制以收集有关新兴风险的最新信息并加以传播,以帮助消除错误信息;
- 在整个组织内迅速传达在风险管理过程中识别出的环境变化和新兴风险;
- 培养快速联系利益相关者的能力以确保双向沟通(例如,提供有关新兴风险的关键信息,获取反馈,使组织能够适应和应对不断变化的情况);
- 建立评估新兴风险人员影响相应决策层的机制,以便在新兴风险达到特定阈值时启动应对计划;
- 建立利益相关者之间的信任(当关键信息不确定、模糊或缺乏处置方案时,尤其具有挑战性);
- 鼓励并授权利益相关者,无论其职位或地位,在察觉可能存在新兴风险时及时告知相关人员。

6.3 范围、环境、准则

6.3.1 范围、环境

除 GB/T 24353—2022 中 6.3 外,以下建议也适用。

组织宜考虑其运营环境的多个方面。风险来源可能产生于组织与社会、地缘政治、环境、经济、技术、法律和伦理等因素的关系、互动或相互依存,以及其内部治理、文化和运营方面。宜采取广阔的视角和长远的时间跨度审视风险来源;微弱信号和早期预警迹象可能出现在直接环境之外。环境信息的广度和深度对于有效管理新兴风险至关重要。

除了解组织当前运营环境外,组织宜寻找可能成为新兴风险源的变化和趋势。环境变化可能由内部因素驱动(如拓展新领域),或外部因素驱动(如新技术)。这些变化可通过关联组织和行业对组织产生直接或间接影响。

环境变化可能是渐进的(如气候变化、阶段性变革、自然灾害),也可能是突发的(如疫情大流行)。在某些情况下,环境变化的可能性本身即可被识别为风险。

宜在运营层面和战略层面评估环境变化的重要性,因为这些变化可能产生重大的战略和运营影响。考虑新兴风险环境时,宜遵循以下建议。

- 新兴风险相关活动的范围宜具有足够的广度,覆盖可能对组织目标构成风险的所有变化。包括政治、经济、社会、技术、法律和环境变化以及组织人力资源方面的变化。
- 明确界定风险评估的边界,包括组织边界、系统边界、流程边界、项目或活动边界。
- 识别并理解可能对组织实现目标能力产生积极或消极影响的外部因素及其变化方式。
- 理解组织内部环境中可能增加新兴风险敏感性和脆弱性的方面。
- 建立监测机制,用于跟踪内外部环境变化,包括渐进性趋势和渐进性变化。
- 制定并分析情景方案,以研判未来可能出现的态势。
- 持续监测组织环境发展方式的变化(不仅是变化本身,还包括在组织环境中的认知变化,这有可能成为新兴风险的来源)。
- 在监测到相关新兴风险时,评估韧性及其指标(见第 7 章)。

组织宜在定期评估内外部环境的基础上,持续开展环境扫描以识别变化。通过动态更新数据,深化对新兴风险特征的理解,为风险持续管理提供有效情报(见第 8 章及附录 E)。

宜使用多样化信息来源以帮助理解新兴风险环境。包括但不限于浏览网页、与行业协会和其他专业机构联系以及非正式专业交流网络。

注:使用 PESTLE(政治、经济、社会、技术、法律、环境)或 STEEPLE(社会、技术、经济、环境、政治、法律、道德)等结构化分析工具,确保全面评估环境各维度的影响因素。

6.3.2 准则

组织宜确立新兴风险重要性的判定准则与简明规则。然而对于新兴风险而言,由于数据不足且存在高度复杂性或模糊性,难以通过简单规则判定其重要性。关于是否需要针对新兴风险采取行动的决策,通常需通过协商方式作出,并综合考虑以下方面的现有证据:

- 对特定后果是否可能发生的置信程度及依据(合理性);
- 后果的性质及其对目标可能产生影响的程度;
- 特定情景发生的预期可能性;

注:发生可能性、合理性以及后果严重程度的不确定性具有显著差异,因此这些术语不可互换使用。

- 后果严重程度及发生可能性评估中的不确定性水平;
- 变化发生的速度;
- 后果可能发生的时间范围;
- 控制措施的可行性;
- 利益相关者的意见。

对于新兴风险,其因果关系往往尚未完全明确。因此,组织宜采用基于预防原则和透明度的决策方法,特别是当某项活动可能对人类健康或环境造成伤害时。

6.4 风险评估

6.4.1 总则

除 GB/T 24353—2022 中 6.4 外,以下建议也适用。

6.4.2 识别新兴风险

对于难以识别和描述的新兴风险,组织在初始阶段往往缺乏相关的既往认知和经验。

环境的变化产生并塑造新兴风险的发展。其潜在来源包括但不限于:全球观念改变、创新技术应用、其他组织行为、政治经济压力以及环境社会变化等。

这些风险可能对多重目标产生正面或负面影响,并引发连锁效应与复合效应,但其影响往往不会立即显现。因此,宜特别注重运用多元方法/技术和信息源,系统识别单一风险源可能引发的各类正面与负面后果。

采用结构化方法识别新兴风险有助于避免重大疏漏,也可适度使用非结构化识别与数据收集技术,以激发创新思维。综合运用多种互补性方法技术,可实现更全面的风险识别。

组织宜:

- 从多个视角或使用相关方法/技术对运营环境进行定期和全面审视,以识别环境变化和新兴风险;
- 在战略层面及全组织范围落实风险管理过程时,主动识别新兴风险(个别项目或部门的重要风险在高层战略思考中可能被忽视);
- 分析可能最终导致新风险的趋势;
- 明确风险来源及相关潜在情景;
- 积极探寻具有正面与负面双重结果的情景;
- 探索相互关联的风险和背景;
- 确定和监测新兴风险指标,以便对即将发生的后果或正在出现的新机遇和威胁发出预警;
- 持续监测数据,以便在获得最新信息时更新风险描述。

GB/T 27921 中用于识别和分析风险的方法同样适用于新兴风险。情景分析法有助于识别前所未

见的后果及连锁复合效应。该方法涉及基于环境特征识别多种可能发展情景,制定响应方案以达成预期未来状态。

促使人们从不同角度思考的方法同样有效。

6.4.3 分析新兴风险

风险分析旨在深入理解风险,以便作出明智决策。宜确保对以下事项有充分了解:

- 新兴风险对组织是否重要(见 6.3.2);
- 组织如何应对新兴风险,以及应对的紧迫性;
- 可用行动方案的选择。

组织宜特别关注初始数据有限、认知存在重大不确定性(如情景可能性、后果或控制措施有效性),或决策信息解读受到认知偏差影响(见附录 D)的新兴风险。此类情况下,组织宜通过权威渠道获取最佳可用信息和数据,并尽可能进行验证。

鉴于新兴风险的特点,组织宜分析新兴风险的来源、潜在事件与情景以及它们对目标的正面和负面影响。同时宜考虑连锁效应和复合效应的可能性。

情景分析法也可用于评估风险应对措施的预期效果。博弈论方法(见 GB/T 27921)可纳入其他利益相关者(假定其基于自己利益行事)的行为考虑。针对每个情景,组织宜考虑对不同目标的影响程度、预期发生可能性以及相关评估的不确定性。

若初始估计存在高度不确定性,可采取以下应对方案:

- a) 通过专家咨询或补充研究来扩展知识;
- b) 采用风险发生可能性区间明示缺失信息(将可能性本身作为随机变量);
- c) 使用类似且更易理解的信息;
- d) 明确传达知识可能基于有限信息或个人感知,以便决策者了解判断基础。

宜记录用于支撑评估的所有数据(见 6.7)。

可通过后果与可能性结合评估风险等级,但决策者有时更需关注后果及其发生可能性的独立信息。宜记录并传达信息及评估中的不确定性。

对于存在以下特征的新兴风险,即使能识别环境变化或早期征兆,仍需特别注意:

- 可能情景尚未明确;
- 因果关系模糊;
- 无法描述或预估后果及可能性;
- 无法全面把握问题的影响范围;
- 不存在单一解决方案。

注 1: 此类风险有时被称为“棘手型风险”。

针对此类风险,宜采取预防性措施,确保控制方案能够在风险态势逐渐明确时动态调整。组织宜尽可能地培养预测、准备、响应和适应意外后果的能力(见第 7 章),同时持续开展信息和数据收集工作(见第 8 章)。对此类风险而言,识别变化的微弱信号尤为重要。

随着更多数据的获取,宜更新情景描述、因果关系、后果与可能性评估以及其他支撑性信息。在此过程中,新兴风险的重要性会发生显著变化。一些新兴风险可能无关紧要,而另一些则可能变得更加重要。随着对潜在情景的不断深入理解,也可能识别出新的风险。

宜明确各情景的时间维度,这将直接影响数据收集和处理的紧迫性。例如:

- 短期新兴风险是指可能已经对组织造成严重后果的风险,这些风险宜立即关注,并分配资源进行数据收集和分析,紧急补充认知;
- 中期新兴风险是指短期内不会产生严重后果的风险,但会随着环境的变化而发展,关键是通过有效的信息解读构建知识体系,识别需较长时间落实的潜在控制措施;

——长期新兴风险是指当前不会对目标产生后果的风险,但环境可能会变化并可能在未来产生重大风险,宜持续监测环境变化,并建立风险重新评估指标。

变化速率宜纳入考量,例如以下方面的变动率:

- 组织环境的变化速率;
- 后果的变化速率;
- 风险情报循环中的风险情报。

注 2: 风险情报成熟度水平可通过“适宜的知识质量”进行衡量(见 E.4)。

除分析单个风险之外,宜考虑风险之间的相互作用。宜探讨变化的环境对已识别风险的影响。宜根据环境变化审查所做的假设,以查看这些风险是否在不断发展。控制措施在新环境中可能无效,宜在可能的情况下进行测试或验证。

6.4.4 评价新兴风险

宜根据风险准则评估分析结果,并综合考虑社会、监管、文化、环境和伦理等方面。在涉及风险的业务决策和权衡取舍时宜考虑新兴风险的重要性。对于某些风险,不需立即作出行动决策。原因包括:

- 没有足够的信息支撑作出任何决策;
- 风险对组织的影响程度较低;
- 风险后果显现周期较长。

此类风险宜持续监测。

新兴风险相关数据、信息与知识的缺失,可能导致对其后果及其发生机制存在重大认知不确定性。在此情况下,采取预防性原则进行风险评估并制定应对措施可能是恰当选择。

人们对风险的认知因目标和偏见而异。这在涉及未知新兴风险以及缺乏评估数据时尤为明显。

在某些情况下,如果潜在后果或其发生可能性存在重大不确定性,确定可能的行动并考虑哪些是可行的和有用的会有所帮助。该方法同样适用于后果极其严重的情况,例如潜在致命后果。

随着新兴风险数据的获取,宜将风险重要性认知的变化纳入组织决策过程。在某些情况下,随着知识的增加,风险指标可能被证实不成立。优先级随后发生变化,监测可能减少或终止。

如果适当,宜在整个组织中传达有关风险的信息,以便在正在作出的决策中考虑这些风险。

组织宜分配责任和权限,以发现和响应有关新兴风险的数据和信息变化,并将其传达给决策者。

6.5 风险应对

针对新兴风险,随着环境演变或认知深化,风险管理措施宜相应调整。组织宜持续评估应对措施的有效性,并根据需要及时优化。鉴于新兴风险的后果与发生可能性往往难以确定,组织宜具备预测、准备和应对多种未知因素,以及适应意外情况的能力。

除 GB/T 24353—2022 中 6.5 外,以下建议也适用。

组织宜:

- 评估新兴风险处置方案;

注: 场景分析法和事件树分析法可用于比较不同处置方案,见 GB/T 27921。

- 将可能对组织产生严重后果的新兴风险纳入业务连续性计划;
- 保持敏捷,不断评估其控制环境,以确定所需行动和应对意外事件的韧性;
- 测试已实施的风险处置措施;
- 将新兴风险应对计划整合至组织的运营和规划流程中。

6.6 监督和检查

除 GB/T 24353—2022 中 6.6 外,以下建议也适用。

组织宜持续有效地监测和衡量风险管理绩效,并审查框架、政策及计划对新兴风险的适用性。

组织宜对新兴风险识别和评估流程实施监控,并定期审查其有效性及改进空间。

由于新兴风险具有动态演变特性,因此持续监测流程产出尤为重要。例如,组织宜监测相关环境、已识别的风险、可用数据和信息、风险的重要性以及正实施的应对措施。进而可及时响应各类变化。

组织宜持续监测环境变化及其影响(见 6.3.1)。宜监测有关新兴风险的数据和信息,以更新对特定问题的理解。宜确定并监测可以指示变化开始发生的指标。

随着对风险的理解不断完善,宜持续监测现有措施和拟议措施的有效性,包括对以往相关经验结果的批判性审查。组织宜建立制度,从新兴风险中吸取经验教训,作为持续改进的一部分。

6.7 记录和报告

除 GB/T 24353—2022 中 6.7 外,以下建议也适用。

新兴风险信息的载体形式、更新频率及报告方式,宜依据组织及利益相关者的实际需求确定。

一般来说,有关新兴风险的记录应用于以下方面:

- 为决策者提供及时的新兴风险动态信息;
- 向组织内外的利益相关者提供新兴风险管理有效运行的保证;
- 在获取信息时,持续记录新兴风险演变过程及控制措施历史数据;
- 跟踪风险管理计划和处置方案的进展情况。

有关新兴风险的记录信息宜包含对风险及其各种潜在情景的描述性信息(见附录 B),如果可用,宜包含有助于理解的验证定量信息。

在管理新兴风险的背景下,一些司法管辖区的法律或监管义务可能要求组织内指定职能或负责人报告新兴风险的管理情况。有关新兴风险的记录信息宜可获取、维护和更新。附录 B 中给出了新兴风险描述或记录模板的示例。

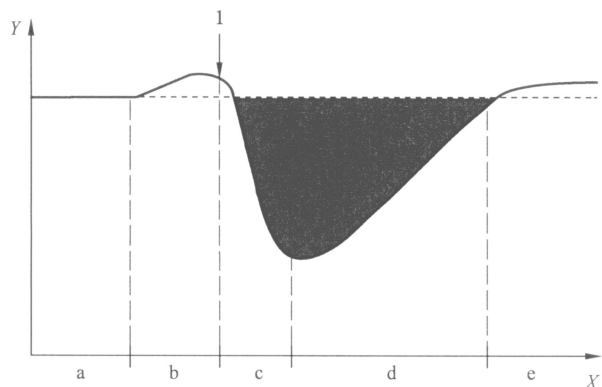
7 通过新兴风险管理提高组织韧性

7.1 能力发展

本文件提供的原则和过程应用于管理新兴风险,有助于组织通过提高其识别环境变化的能力来提高韧性,这些变化可能是潜在新兴风险的微弱信号或早期预警。

组织宜通过收集可用数据并开展支持信息有效解读的分析,获取新兴风险决策所需的关键知识,从而提升自身对不断变化形势的预测、响应和适应能力。宜基于现有数据和信息制定新兴风险情景,以便更清晰地理解新兴风险的发展态势与破坏性事件对组织功能的影响程度之间的关联关系。

图 1 中展示了新兴风险演变场景的示例,该情景通过“从新兴风险出现初期预警到组织实现功能恢复的时间跨度”和“组织对新兴风险负面影响的预见、准备及响应能力”两个维度,展现了组织功能丧失与恢复的动态过程。



- 标引序号说明：
- X —— 情景时间跨度；
 - Y —— 功能；
 - 1 —— 新兴风险/事件/情景的开始；
 - 2 —— 功能丧失；
 - a —— 审视新型风险；
 - b —— 预期/准备；
 - c —— 吸收/承受；
 - d —— 响应/恢复；
 - e —— 适应/转型。

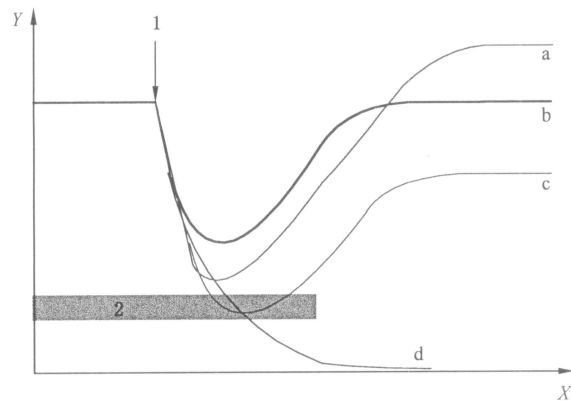
图 1 新兴风险演变场景的示例

组织的韧性能力将决定从破坏性事件到恢复各个阶段所需的时间，以及对组织功能损失的程度和随后的恢复程度。而组织对变化环境的适应能力及其化危为机的前瞻性，往往体现为干扰性事件后组织功能的超越性提升。图 2 同样展示了破坏性事件造成的损失和恢复程度之间的关系，以及韧性属性和组织能力对以下潜在结果的影响（见图 2）：

- a) 事件后功能水平超越事件前状态（适应能力）；
- b) 功能恢复至事件前基准（业务连续性能力）；
- c) 功能未达事件前基准（能力受限）；
- d) 丧失最低必需功能并引发系统停摆（能力不足）。

不断审视多种情境将有助于组织更好地理解新兴风险，并为构建、评估与强化组织韧性属性提供必要的知识储备。

这些组织属性可帮助识别和分析新兴风险及其特征的变化，可缩短从早期预警到破坏性事件爆发的响应窗口期，又可提升组织启动响应措施并适应环境变化的敏捷度。韧性能力建设/提升应采取主动式策略（例如通过系统抗压测试实现能力优化）。



标引序号说明：

- X —— 情景时间；
- Y —— 功能；
- 1 —— 新兴风险/事件/情景的开始；
- 2 —— 压力测试极限；
- a —— 功能较之前更好；
- b —— 功能与之前相同；
- c —— 功能仅部分恢复；
- d —— 功能完全丧失。

图 2 事故(事件)对功能的潜在影响

韧性组织宜具备吸收并适应环境变化的能力,这种适应性不仅涵盖风险性变化,更包含潜在机遇性变革(例如应对突破性创新或颠覆性创新的场景)。组织宜准备好预测、应对和适应此类创新引起的变化,无论其源于组织内部还是市场环境(例如,能够抓住创新带来的机会以获得竞争优势)。增强韧性也宜被视为对不可预见风险的一种预防措施。

7.2 新兴风险和韧性指标

新兴风险可能呈现出某些特征,这些特征不仅会削弱组织在动态环境中的吸收与适应能力,还将对组织韧性属性的其他方面产生影响,具体包括(但不限于)以下层面：

- a) 愿景、目标和核心价值观；
- b) 战略问题的决策制定；
- c) 在重大不确定性期间的领导力；
- d) 行为、创造力和创新的文化；
- e) 信息解析与知识转化应用能力；
- f) 资源分配和部署；
- g) 网络 and 关系；
- h) 协调管理新兴风险所涉及的各个领域；
- i) 维持系统和过程持续改进的能力。

新兴风险蕴含的重大不确定性亦可能改变上述韧性属性的构建、采纳及实施环境。而这种环境变迁对组织现有预见、规划、响应及适应能力的冲击程度,则作为组织韧性的滞后性指标存在。

组织宜在检测到新兴风险后果前,通过持续监控韧性属性并针对潜在新兴风险情景开展压力测试,以此评估自身韧性水平。此类情景的构建可基于初步数据分析及对多源组织环境的持续监测来实现。

当组织遭遇与新兴风险相关的重大破坏性事件时,应参照图 2 及以下组织韧性示例性指标体系评估其韧性属性的有效性。

——时间依赖性指标：

- 环境变化到识别新兴风险的时间间隔；
- 风险识别到相关事件发生的时间间隔；
- 新兴风险事件触发到功能开始丧失之间的时间间隔；
- 对组织目标影响的持续时间；
- 事件发生到恢复至事前状态的时间间隔。

——生产力与绩效指标：

- 不同程度功能丧失速率；
- 丧失程度百分比；
- 功能丧失持续期；
- 机遇响应效能；
- 功能丧失对组织目标的影响。

——核心韧性指标：

- 愿景、目标、宗旨及价值观的可持续性；
- 从新兴风险中实现机会的程度；
- 持续增强准备、吸收、响应、恢复和适应/转型能力。

——组织宜采用利益相关者达成一致的韧性指标，这些指标宜：

- 整合专家研判(定性)、测量数据及大数据(定量)等多源信息输入；
- 使组织的韧性属性(特别是关键指标)能够进行基准测试，并由相关利益相关者达成一致；
- 确保跨行业参与方之间的通信与技术系统互操作性及透明度；
- 全面、清晰且无歧义地描述韧性属性。

组织宜将韧性指标应用于评估其应对新兴风险的韧性水平，并将其纳入相关的风险情景、压力测试和演练要求中。附录 F 给出了韧性指标的示例。

8 风险情报循环和新兴风险管理

8.1 概述

新兴风险情报获取的步骤流程如图 3 所示。情报工作可在战略、战术和操作 3 个层面展开，情报宜被应用于构建并强化组织对新兴风险的认知储备与决策支持能力。

新兴风险宜通过风险情报循环实现有效管理，其实施路径包括：

- 在具有不可预测波动性、高度不确定性、网络复杂性及快速变化特征的环境中，持续扫描、采集、分析和解译新兴风险的数据、信息和知识；
- 考虑到在这种不断变化的情况下采集到的新兴风险数据通常是有限的(在质量和数量方面)，且紧急解译往往导致可用信息模糊性递增；
- 考虑整合既有已知风险数据；
- 鉴于新兴风险可用数据和信息的有限性，宜明确情报质量与决策效能的直接关联。

风险情报循环的运作效能、原则及实施流程见附录 E。

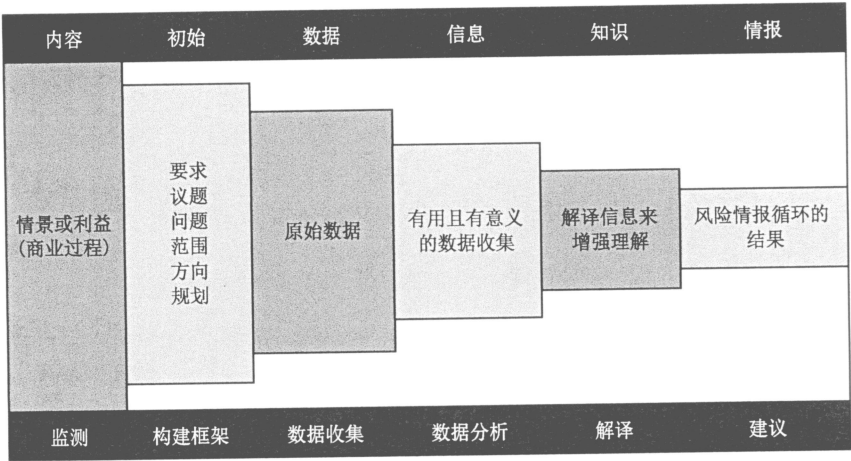


图 3 数据—信息—知识—情报(DIKI)流程

8.2 将知识应用于新兴风险决策

组织宜在 GB/T 24353—2022 给出的风险管理过程的每个步骤中,将风险情报循环获取的知识系统化应用于新兴风险管理各环节。随着新兴风险数据置信度的持续提升,知识与情报质量将系统性增强 GB/T 24353—2022 给出的风险管理过程中各环节的新兴风险决策效能(见第 6 章,图 4 和图 E.1)。

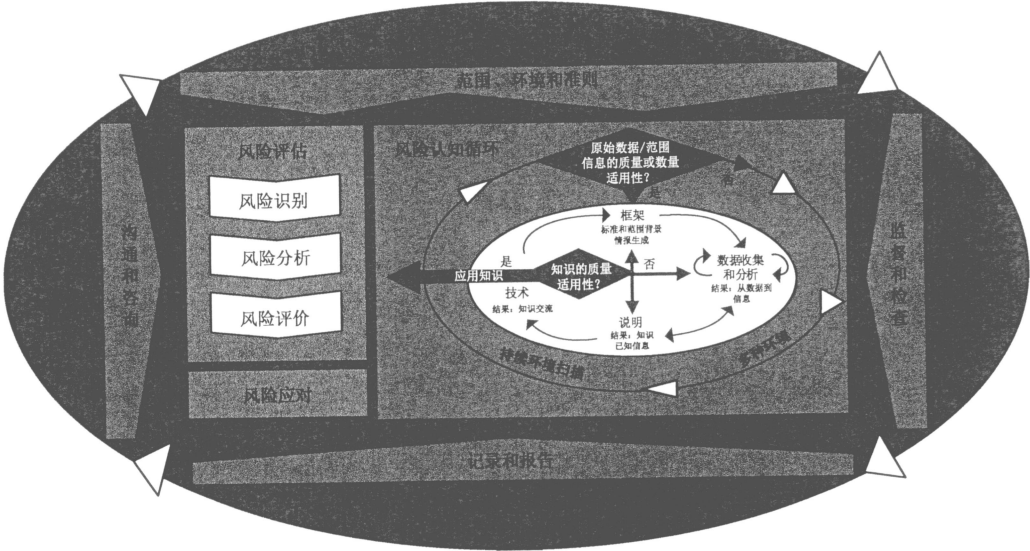


图 4 应用于 GB/T 24353—2022 的新兴风险的风险情报循环

决策层,包括最高管理者和风险责任人,宜在风险管理过程中持续应用此类情报,以预测情境变化趋势,并就新兴风险应对策略作出及时、明智的决策。同时,宜重视对新兴风险累积知识的验证工作。在验证信息如何转化为知识时,宜考虑人类判断中固有的不确定性以及个人感知中潜在的认知偏差(见附录 D)。这种不确定性反映了动态环境对决策的影响,可能导致未知或不确定的结果。

鉴于新兴风险的高度不确定性,DIKI 过程(见图 3)应采用迭代方法,并在每个环节进行验证,因为新出现的问题往往需要额外验证。

将预见性方法(见 6.4.4)与风险情报循环结合使用,以增强新兴风险管理的有效性。

在应用风险情报循环的同时,采用预防性方法可增强新兴风险管理的有效性。在应用知识循环时,宜主动寻求协作和信息共享机会。管理新兴风险的系统方法还宜考虑相互作用和相互依赖。宜与所有可能受到组织环境变化影响及受特定变化直接影响的利益相关者共享信息。

附 录 A

(资料性)

可能成为新兴风险来源的情境变化示例

以下情境变化可能成为新兴风险的来源。

- 自然灾害(极端天气事件):如 2024 年 9 月,超强台风“摩羯”袭击亚洲多国,包括菲律宾、中国和越南,造成大量人员伤亡和经济损失。
- 物联网(IoT)的挑战(网络安全):物联网将彻底改变数字世界。对于能够通过智能化、自主化和互联化改造其产品、服务和流程的韧性企业而言,这场数字革命带来了广泛机遇。然而,这些机遇也伴随着威胁。连接性和对数字流程依赖度的增加,引发了关于网络和数据安全、可靠性、长期维护及软件更新的问题。系统故障和黑客与犯罪分子的恶意攻击可能会导致损失。由于缺乏一致的跨国法规标准,还可能存在法律和合规风险。
- 抗菌药物耐药性(健康):当微生物(如细菌、病毒、真菌和寄生虫)发生变异,导致某些药物失去疗效时,即产生耐药性。当微生物对多数抗菌药物产生耐药性时,通常被称为超级细菌。这一问题至关重要,因为耐药感染可能造成重大的人员伤亡和经济损失。
- 人工智能缺乏透明度:随着人工智能(AI)和认知计算的进步,机器可以开始代表人类作出决策。决策权的转移以及透明度或人类监督的缺失,可能导致意想不到的风险或不可预测的结果,从而产生复杂的责任问题。此外,与 AI 相关的理论、社会和市场问题也越来越突出。
- 自主机器(网络安全、AI):由于机电一体化、快速学习和 AI 的进步,自主机器发展迅猛,影响着大多数行业、军事和日常生活。自动驾驶汽车尤其受到关注,这很可能改变各种保险业务的风险格局。
- 气候变化转型风险(气候):随着全球努力适应气候变暖并减少温室气体排放(特别是二氧化碳),转型风险应运而生。这对保险公司在产品设计和相关责任以及投资方式方面都有影响。其中一项特定的转型风险是搁浅资产。即由于政策变化(如煤炭行业、柴油车辆)或碳定价(如过剩飞机)而过时的资产。

附录 B

(资料性)

新兴风险描述或记录模板的示例

附录 B 中给出的示例和列表并非具有详尽性、限制性或规定性。针对新兴风险宜持续采集下列信息。

- a) 新兴风险概念的明确标识(如自动分配的 ID 编码)。
- b) 与来源相关的元数据:作者、时间、组织等。
- c) 新兴风险概念名称。
- d) 可能情景的描述(风险故事),包括与其他风险的关联性。
- e) 预评估结果,涉及:
 - 1) 影响特征,包括正面的和负面的(如系统性、累积性、连续性损失、潜在收益等);
 - 2) 地理与时间数据(风险出现的区域和时段);
 - 3) 治理、沟通、政策、技术等;
 - 4) 生命周期阶段(哪个阶段,如衰退期);
 - 5) 受影响的人类活动领域(如能源、交通);
 - 6) 可能的经济及其他影响(正面和负面);
 - 7) 风险责任人;
 - 8) 知识强度(新兴和成熟程度);
 - 9) 可能适用的评估方法和工具;
 - 10) 相关评估指南或法规(如有);
 - 11) 潜在风险与韧性指标。
- f) 评估信息及评估结果,包括:
 - 1) 新兴风险的来源、潜在情景及其相互关联性;
 - 2) 后果(包括正面和负面影响)的描述,适当时宜说明影响程度;
 - 3) 已实施管控措施的有效性及其效率;
 - 4) 情景及后果发生的可能性/合理性信息;
 - 5) 可能的时间跨度、变化速度及演变速率;
 - 6) 分析所依据的文献及信息来源;
 - 7) 在变化环境中可识别的机遇和威胁;
 - 8) 采用的分析方法、工具及相关输出报告;
 - 9) 数据分析与信息解读方面的不确定性;
 - 10) 可能存在的微弱信号或早期变化迹象。
- g) 建议的治理行动,包括时间安排和责任归属。
- h) 剩余风险。
- i) 监测环境变化及更新新兴风险信息机制。
- j) 参考文献、相关案例及知识依据。
- k) 详细说明文件的引用索引。

附录 C

(资料性)

系统性风险

许多新兴风险具有系统性特征,其起源和演变于紧密耦合的动态系统网络中,这正是当代多元化社会的主要特征之一。“系统性风险”这一概念强调了当今组织面临威胁的相互关联性。经济合作与发展组织(OECD)采用“系统性风险”这一分类,用以描述威胁社会关键系统(如基础设施、医疗保健和电信)的新兴风险。系统性风险是指从区域蔓延到国家乃至全球层面的风险现象。

系统性风险可通过以下 5 个特征区别于其他风险类型。

- a) 系统性风险具有高度复杂性特征。在分析系统性风险时,因果关系难以厘清。一方面源于所涉系统(如关键基础设施、企业、生态系统及其组成部分)的固有复杂性。另一方面则因系统性风险可与传统风险(如自然灾害)相叠加。
- b) 系统性风险具有跨界和跨部门特征。尽管其源头可追溯至特定系统或事件,但其连锁反应会向其他系统扩散,产生进一步的影响。因此,这对基于隔离和分割的传统风险分析和治理构成挑战。
- c) 由于存在非确定性因果关系,系统性风险以非线性方式发展。其典型表现是已知风险因素与随机演变或处于可测算性边界的未知诱因相互交织。
- d) 多数系统性风险具有与临界点(或临界期)相关的非线性关系。一旦达到临界点,受影响系统将在短时间内发生生存条件的剧变。
- e) 对于系统性风险可能造成的毁灭性影响,监管措施和公众认知往往存在滞后性。尽管气候变化等部分系统性风险已引发公众关注,但利益相关者和民众普遍认为相关管理政策存在零散性、不足性和不协调性。

组织宜关注系统性风险的以下特性,尤其是:

——相互依赖性;

——干预因素、不确定性与非线性关系构成的复杂结构,这要求采用系统性方法管理新兴风险。

组织宜为新兴风险的不可预见压力因素以及新兴风险可能造成的级联或复合效应做好准备。为实现预防、减轻或应对系统性威胁的目标需建立高效、整合且包容的治理策略。特别是在风险评估以及风险管理过程中,宜考虑利益相关者或公众的关切。

附录 D

(资料性)

可能影响管理新兴风险的因素示例

可能影响新兴风险管理的因素示例见表 D.1。

表 D.1 可能影响新兴风险管理的因素示例

因素	详细解释和注释
与普通感知、沟通相关	
错误感知和错误解释	机会或利益的可能误解；易受故意或其他误解的影响
假阳性	假阳性对评估结果的影响
假阴性	假阴性对评估结果的影响
(全球)灾难潜力	如果大量人员在单个事件中死亡，而不是分散在时间上的小量死亡，我们对风险的感知就会提高
敏感度	对单个事件(例如事故)的风险感知的敏感度，公众感知的波动性
沟通不畅	新兴风险的沟通可能是风险水平感知的一个因素，因为根据定义，可用知识较弱；在极端情况下，沟通不畅本身可能成为一种风险
单个个体的感知水平	
缺乏熟悉感	陌生或新颖的风险会让人更加担心
缺乏理解	如果一个人认为某项活动或技术的工作原理不太清楚，他/她对风险的感知会增加
缺乏个人控制或自愿性	如果一个人觉得潜在的危害超出了他/她的控制范围(比如乘坐飞机的乘客)，他/她会比觉得自己处于控制之下(比如作为车辆驾驶员)更担心；或者无法决定个人是否要冒险，风险感会更具威胁性
涉及未来世代的风险	如果风险涉及未来世代，人们往往会认为这更具相关性并且容易被社会加强
影响人的身份	受影响的人能够具体化风险后果，相对于抽象的统计数据，更容易感知风险的增加
可怕的预期	如果风险的后果会产生恐惧，那么风险感会增加
缺乏信任	如果相关机构不受信任，个人的风险感知通常会增加
缺乏公平性	如果某些人获得了好处而其他人承受了不利后果，那么人们会提高风险等级
缺乏可逆性	如果某种结果的影响无法逆转，风险感会增加
个人风险	如果风险涉及自己(非自愿性)，相对于平均水平，人们倾向于认为风险更高(除非我们认为自己比其他人更能控制风险)
认知偏见	诸如确认偏见等认知偏见，包括信息疲劳等，可能会显著影响新兴风险及其感知
与新兴风险治理相关的内容	
授权	授权或认证计划的可用性(逐步授权)
映射	可能进行映射(例如在地理或上下文地图上)

表 D.1 可能影响新兴风险管理的因素示例（续）

因素	详细解释和注释
管理	可能进行管理,特别是后果管理
保护或预防措施	可能设想实施保护或预防措施
社会动荡	可能引发或导致社会动荡的潜力
涉及全球新兴风险管理的内容	
无法观察或监测的情况下	如果监测到的虚假信号非常高,则有可能监测到风险
无法控制或减轻的情况下	缺乏固有的管理、控制或计划减轻机制
易受无知影响	现代世界的复杂性通常导致人们对某一现象或问题(例如计算机)的信息泛滥,但缺乏对该现象的基本理解

附录 E
(资料性)

管理新兴风险的知识和风险情报循环

E.1 引言

新兴风险管理依赖于获取最佳可用信息,以便获得、分享和传达情报,作为战略决策的输入。情报是收集、分析和解释数据、信息和知识的结果。数据、信息、知识和情报之间的关系(DIKI)在第 8 章中显示(见图 4)。

在战略层面上,情报为高层管理层提供输入,使他们能够作出决策,影响组织的愿景、战略、政策和目标,以及与预期或可想象的新兴风险相关的组织内决策。

在操作层面上,情报面向决策者,使他们能够作出影响新兴风险和其控制下的相关风险以及特定价值链的决策。

组织宜采用和应用风险情报循环来开发有关管理新兴风险的知识和情报,这与 GB/T 24353—2022 给出的风险管理过程一致,以便将有关新兴风险的知识传达给负责、有责任 and 权力来管理风险的人员。

风险情报循环的关键要素包括下面阐述的步骤。

E.2 风险情报循环和管理新兴风险

风险情报循环应用于新兴风险时,为第 6 章中描述的新兴风险管理过程的沟通和咨询方面建立了基础,并由两个相互关联的迭代循环组成(见图 E.1)。

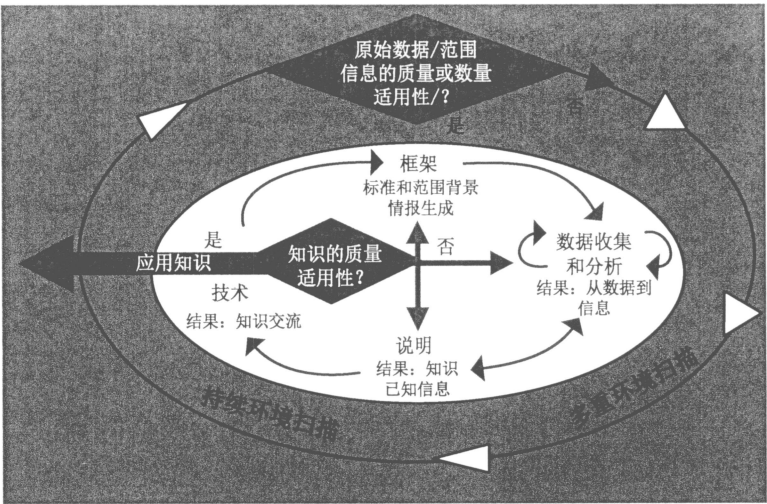


图 E.1 新兴风险的风险情报循环

E.3 多重环境扫描(外部循环)

持续扫描组织环境的多个方面,有助于识别数据、情况和/或行为中的微小变化,这些变化之间的时间间隔,以及它们对组织及其目标的可能影响。在系统性审查(GB/T 24353—2022 过程的监测和审查阶段)期间识别到环境中微小的变化和观察到的变化率,可能意味着对组织目标潜在新兴风险的早期警告或指标,这些风险涉及威胁或机遇。

多重环境扫描(见图 E.1)可提高对环境中已识别变化的可用数据的质量和数量,作为内部情报循

环的进一步输入。

E.4 风险情报流程(内部循环)

E.4.1 总则

风险情报流程的内部循环包括以下 4 个步骤,具体解释如下。

E.4.2 制定框架

新兴风险的框架制定阶段包括以下几个方面的内容。

- 通过情报循环确定所需的知识范围,即风险所有者希望了解(更好的)什么,以及如何和为什么了解。
- 定义与背景变化相关的外部和内部问题。
- 确保情报循环与业务流程的关键方面/关系相一致,其中背景变化表明可能存在潜在风险或新兴风险。
- 建立标准用以定义:
 - 数据收集和分析的边界;
 - 信息的解释和知识的生成;
 - 知识的传播以及向决策提出建议(从新知识中得出的可能行动);
 - 后续阶段的时间、成本和质量计划。

E.4.3 数据收集和分析

新兴风险的数据收集和分析步骤可以分为两个阶段:数据收集和验证阶段,以及数据分析提取信息阶段。

数据收集和验证阶段包括识别和选择数据和信息来源,查找和挖掘数据和信息,检查和维护质量和数量,以及识别准备解释的模式。

该阶段旨在生成准备好进行分析的且经过验证的数据和信息。这些数据和信息可来自内部或外部来源。通过考虑可靠性和准确性以及适用性和充分性来评估数据和信息的质量。

可通过对数据进行测试运行来进行数据验证,包括但不限于:

- 数据一致性、准确性、相关性、充分性和可靠性;
- 未使用、杂乱无章或不一致的数据;
- 敏感性分析;
- 异常值的识别和处理。

数据分析将一组原始数据转化为一组有用的信息。该子阶段使用在框架期间确定的分析工具,从各种来源的原始数据中生成复合信息(例如,相关性、趋势、地图、序列、聚类、模式)。分析可通过基本操作进行组织,例如,选择、分类、抽象、分解、规范、比较、对应、实例化、相关性和转换。

常用的自动化工具可处理大量数据和信息,可用于揭示模式和趋势,或者提供可视化表示,例如,统计工具或软件、数据挖掘、制图和可视化工具、分类、分类法或词汇或语义分析。

E.4.4 信息解释

在此阶段,信息是从组织环境中收集和处理的的数据中产生的,并且可能是潜在风险的前导指标,需要进行解释和转化成有意义和有价值的信息以生成知识。

对早期或薄弱信号的数据进行解释,了解环境和情况的变化以及可能出现的潜在问题,可协助生成足够的知识,为应对新兴风险制定可能的情景。

当观察到系统和组织环境中的微小变化时,这些变化需要进行解释,以了解变化背后的“如何和为什么”。环境变化的性质和原因受到个人风险感知的影响。

系统和组织环境中的微小变化和数据可能会提示出潜在问题或具有重大后果,例如潜在风险的早期警示或薄弱信号。这些解释可基于个人对风险的感知,形成于教育、理性和逻辑或类似的过去经验和主观判断。

解释的结果是有助于管理风险和作出决策的知识。例如:

- 竞争对手活动的薄弱信号可被解释为业务流程的机会和/或威胁;
- 确定技术发展的优先事项,可被解释为运营的优势和/或劣势;
- 重新评估支持实现既定任务的路线图的知识体系。

解释和数据收集/分析之间的反馈和迭代取决于具体情况,例如添加或修改数据集,应用不同的分析工具,避免任何可能的错误解释。

E.4.5 情报——应用于对新兴风险决策的知识传达

提高对新兴风险的认知取决于如何将有关变化情况的情境化数据转化为有用和清晰的信息,并向决策者传达(例如,以情景的形式)。

对新兴风险的认知是对验证信息的解释结果。新的认知解释了对组织环境中意外变化的理论和实践方面的贡献,以及新兴问题转化为新兴风险的潜力。通过情境扫描、观察和学习的迭代过程,对新兴风险的显式和隐式认知将不断发展,帮助决策者确定新兴风险事件或现象的可能性和后果。

组织知识的增长宜平衡变化带来的不确定性和复杂性的增加。增加的知识宜使组织能够更好地理解与情境变化相关的不确定性和复杂性,并有机会确定潜在的新兴风险情景、其原因、后果以及如何控制它们。

在上述内部循环的第4个步骤(见图 E.1)中,如果有足够的信心则可对“知识质量是否合格?”这个问题给出肯定的答案:

- 所做的假设被认为是合理的;
- 可用足够数量的可靠和相关的数据/信息;
- 所涉及的现象已被理解;
- 所使用的模型已知能够提供所需的准确预测;
- 专家之间存在共识。

随着对新兴风险的可用数据和信息的信心增加,知识和情报的质量将有助于增强对新兴风险的决策能力和提高韧性。

附录 F
(资料性)
韧性指标模板示例表

韧性指标模板示例见表 F.1。

表 F.1 韧性指标模板示例表

指标	按计划完成的应急演练百分比
描述:整个演习计划按照定义的截止日期完成。为了进行跟踪,进行测量。如果计划未能实现,存在未受过训练的人在紧急情况下无法适当响应的风险	
建议的测量尺度	〈高〉 ≥95% 〈中〉 85%~94% 〈平均〉 75%~84% 〈低〉 ≤74%
特征	比例, %
状态	☒建议的 ☒详细阐述的 ☒已接受的本地案例研究 ☒验证过的 ☒事实或工业标准 ☒标准 ☐法规的一部分 ☐用于基准测试
提供者或建议者	××专业类协会
相关的功能性或业务性测试(是或否)	是
适用于特定应用(比如:关键基础设施)	所有基础设施 ☒医疗保健系统 ☐工业生产系统 ☐信息和通信技术系统 ☐金融系统 ☐交通系统 ☐水供应系统和其他重要基础设施 ☐能源供应系统 ☐其他
适用于或与以下威胁相关	☒所有或任何威胁 ☒网络攻击 ☒社会动荡 ☒级联效应 ☒恐怖袭击 ☒自然威胁 ☒新技术事故 ☒其他威胁

表 F.1 韧性指标模板示例表（续）

指标	按计划完成的应急演练百分比
适用于或与以下阶段相关	☐理解风险 ☒预见或准备 ☒吸收或承受 ☒响应或恢复 ☐适应或转化 ☐理解风险

参 考 文 献

- [1] ISO 2231 Rubber-or plastics-coated fabrics—Standard atmospheres for conditioning and testing
- [2] ISO 56000:2020 Innovation management—Fundamentals and vocabulary
- [3] ISO 56006:2021 Innovation management—Tools and methods for strategic intelligence management—Guidance
- [4] Key, J., King, M. Radical uncertainty—Decision—making for an unknowable future. The bridge Stress Press, 2020.
- [5] Russoa, D., Ciancarinia, P. A Proposal for an Antifragile Software Manifesto, Procedia Computer Science, 2016, 83, pp.982-987.
- [6] The UK Government Resilience Framework, UK Cabinet Office, 19 December 2022. Available from: <https://www.gov.uk/government/publications/the-uk-government-resilience-framework>
- [7] European Union, DRS-14-2015: Critical Infrastructure Protection topic 3: Critical Infrastructure resilience indicator-analysis and development of methods for assessing resilience. In: Horizon 2020 Work Programme 2014-2015: Secure societies-Protecting freedom and security of Europe and its citizens. EU, 2015. Available from: https://ec.europa.eu/research/participantsdata/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_en.pdf.
- [8] DIN-SPEC 96461 Stress-testing resilience of critical infrastructures exposed to cyber-physical threats
- [9] DIN CWA 16649, DIN SPEC 91299: Managing emerging technology-related risks
- [10] International Risk Governance Council (IRGC). Improving the Management of Emerging Risks: Risks from new technologies, system interactions and unforeseen or changing circumstances Geneva: IRGc, 2011. Available from: <https://irgc.org/wp-content/uploads/2018/09/irgcer2conceptnote2011.pdf>.
- [11] CEN/CENELEC Standards-Innovation Bridge, iNTeg-Risk Early Recognition, Monitoring and Integrated Management of Emerging, New Technology related Risks (Risk Radar), EU FP7 project, <http://www.integrisk.eu-vri.eu/>.
- [12] IRGC The Emergence of Risks: Contributing Factors. Geneva: IRGC, 2110. Available from: https://irgc.org/wpcontent/uploads/2018/09/irgc_ER_final_07jan_web.pdf.
- [13] USGS. Overview of the ARkStorm Scenario. Prepared for the US Geological Survey Multi-hazards Demonstration Project. USGS Open File Report 2010-1312, 2011.
- [14] Center for Chemical Process Safety (CCPS). Guidelines for Risk Based Process Safety. Wiley, 2007. ISBN: 978-0-470-16569-2.