ICS 03.100.01
CCS A 02

中华人民共和国国家标准

GB/T 27914—2023
代替 GB/T 27914—2011

风险管理　法律风险管理指南

Risk management—Guidelines for the management of legal risk

（ISO 31022:2020,MOD）

2023-08-06 发布　　2023-08-06 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。

本文件代替GB/T 27914—2011《企业法律风险管理指南》。与GB/T 27914—2011相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“风险”“法律风险”“组织”3个术语（见3.1、3.2、3.3），删除了术语“企业法律风险”（见2011年版的3.1）；

b) 更改了“原则”的数量和内容，增加了“原则”的示意图（见第4章，2011年版的第4章）；

c) 更改了第5章的结构和内容，5.5和5.6合并为一条（见5.5，2011年版的5.5、5.6）；

d) 删除了6.6（见2011年版的6.6），更改了第6章内容（见6.6，2011年版的6.7）。

本文件修改采用ISO 31022：2020《风险管理　法律风险管理指南》。

本文件与ISO 31022：2020的技术差异及其原因如下：

a) 更改了术语“法律风险”的定义（见3.2），删除了术语“法律”，符合我国国情；

b) 更改了第4章“原则”的内容[见第4章的d)和i)]，符合我国国情；

c) 更改了第5章的内容（见5.2.1、5.2.4、5.3、5.4），更加清晰阐述了法律风险管理的过程，符合我国实践；

d) 更改了第6章的内容（见第6章），有助于法律风险管理的实施，符合我国实践。

本文件做了下列编辑性改动：

a) 更改了附录C的内容（见附录C）；

b) 更改了附录D的内容（见附录D）。

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：中国标准化研究院、蒙娜丽莎集团股份有限公司、江苏核电有限公司、中国核能电力股份有限公司、北京大成律师事务所、北京赛尼尔风险管理科技有限公司、第一会达（北京）数据技术有限公司、首约科技（北京）有限公司、北京大成（上海）律师事务所、中共中央党校（国家行政学院）、北京大学、中国矿业大学（北京）、法天使（北京）科技有限公司、广东卓建（中山）律师事务所、云南禾胤律师事务所。

本文件主要起草人：高晓红、陆小伟、张毅、张鹏、徐永前、叶小忠、闫丽萍、王志华、陈立彤、施颖、吕多加、崔艳武、吴倩、华春翔、徐涵、王雷、孙保均、张旗康、游志斌、刘新立、常金光、何力、浦壹婷、郑文杰。

本文件及其所代替文件的历次版本发布情况为：

——2011年首次发布为GB/T 27914—2011；

——本次为第一次修订。

引　言

组织在包含各种法律风险的复杂环境中运行。随着法律、法规体系的不断完善，世界各国对组织的法律监管要求都日趋严格，而且不同国家的法律和监管要求各不相同。不仅如此，面对法律和监管环境的变化，组织需同步适应。尤其在开展新的活动和业务时，组织更要充分考虑各方面的需求。组织在做出可能产生重大法律后果的决定和行动时，面临相当大的不确定性，尤其是重大法律风险对组织的发展影响巨大，使得组织需加强法律风险管理。法律风险管理有助于保护和增加组织的价值。

本文件为协助组织有效地评估和应对法律风险提供指导，旨在帮助组织及其最高管理层：

——实现组织的战略成果和目标；

——鼓励采取更为系统和一致的方法进行法律风险管理，并全面识别和分析问题，以使法律风险得到积极、适当的应对，并获得最高管理层的支持；

——更好地了解和评估法律问题、法律风险的范围及影响程度，并进行适当的尽职调查；

——识别、分析和评价法律风险，为科学决策提供系统方法；

——鼓励寻求持续改进的机会。

需注意，本文件内法律风险的定义是广泛的，在中国的实践中，法律风险一般可分为：法律环境变化风险、违规风险、违约风险、侵权风险、怠于行使权利的风险、行为不当的风险。

本文件：

——为法律风险管理提供指导，使其与合规活动相匹配，并为组织满足其义务和目标提供保障；

——可适用于所有类型和规模的组织，通过提供更结构化和一致的方法来管理法律风险，使组织及其利益相关者在整个过程中受益；

——为法律风险的识别、分析和评价提供综合管理方法；

——支持和补充现有的方法，通过针对组织可能面临的潜在问题提供更好的信息和更深刻的理解，来增强现有方法的效用；

——支持组织可能实施的任何管理流程，例如合规或其他管理系统。

使用本文件的组织将受益于改进商业和运营成果，如提高声誉、改善员工忠诚度、改善利益相关者关系、增强资源与能力之间的协调作用等。

风险管理　法律风险管理指南

1　范围

本文件作为 GB/T 24353 的补充，为组织管理其面临的法律风险提供指南。

本文件提供了管理法律风险的通用方法，不针对某特定行业或领域。组织可根据其具体环境，有针对性地应用。

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

3　术语和定义

下列术语和定义适用于本文件。

3.1

风险　risk

不确定性对目标的影响。

注 1：影响是指偏离预期，偏离可以是正面的和/或负面的，可能带来机会和威胁。

注 2：目标可有不同维度和类型，可应用在不同层级。

[来源：GB/T 24353—2022，3.1，有修改]

3.2

法律风险　legal risk

由法律、法规以及合同事项导致的**风险**(3.1)。

3.3

组织　organization

为实现目标，由职责、权限和相互关系构成自身功能的一个人或一组人。

注：组织的概念包括个体经营者、公司、集团、商行、企事业单位、权力机构、合伙企业、慈善组织或研究机构，或上述组织的部分或组合，无论是否为法人组织，公有的或私有的。

[来源：GB/T 35770—2022，3.1，有修改]

4　原则

法律风险的有效管理需遵循 GB/T 24353 所述的价值观和原则，如图 1 所示：

图 1　原则

以上风险管理的八项原则在法律风险管理环境下体现为 a)～h)所列示的内容。此外，进行法律风险管理，还需考虑“公平”原则，见 i)。

a) 整合：法律风险管理是组织全面治理和管理的有机组成部分。法律风险管理活动需融入组织的战略规划、业务决策和管理流程中。为将法律风险管理融入组织程序和活动，需在组织内确立适当的角色及其职责。法律风险管理需与合规、安全、质量和内部控制等其他管理体系相融合。在评估法律风险和选择应对方案时，宜同时咨询法律问题专家及其他专业人士。

b) 结构化和全面性：在遵循一般风险管理程序的同时，宜使用全面且连贯的方法来管理法律风险。

c) 定制化：组织需根据其内、外部环境的不同，有针对性地开展法律风险管理。其中，外部环境包括法律环境、监管环境和行业特点，内部环境包括法律实体的性质、组织目标和价值观。

组织需详细了解法律的适用性和不遵守法律的影响及后果，确保充分认知和理解新制定或修订的法律，并评估其影响。

组织需尽量降低法律程序在组织内部实施的复杂性和成本，并尽量控制法律风险的负面影响。组织可积极寻求机会，通过在不利事件发生前或可能发生前采取应对法律风险的行动，从而避免纠纷或诉讼，或尝试以平衡成本、商业目标、商誉和组织投入的时间的方式达成和解。

d) 包容性：通过让所有利益相关者参与法律风险的管理，组织可以减少不利事件，包括监管执法措施。各方人员宜分工负责，以形成法律风险管理的长效机制。

e) 动态性：组织需监测并适应法律、公共政策以及运营环境的变化，并建立适当的预警指标。

f) 最佳可用信息：为有效管理法律风险，除内部法律顾问的经验外，在有条件的情况下还可使用商业情报、商业分析、法律数据库和系统(包括案例管理)、电子文件管理工具和服务等。必要时，可以使用外部律师事务所、服务提供者或顾问提供的专业意见。

g) 人和文化因素：考虑到利益相关者可能对法律风险有不同的理解、预期和观点，并且这些观点的建立和认知可能受情感、社会、文化和政治因素的影响，组织可建立正式和非正式的机制以确保人和文化因素不会导致负面的法律风险。组织还需设法鼓励对这类风险进行管理并获得

利益和机会。组织中的每个成员都宜知晓其作为或不作为是如何影响法律风险的。

h) 持续改进：组织需综合考虑经验教训、过往交易评审意见、最佳实践、来自内部和外部顾问的专业建议、内部审计以及适用法律的变更等，并在此基础上采取行动。

i) 公平：对决策者而言，确立公平原则，可指导法律风险的管理，兼容利益冲突的管理，并在决策中提供公正、独立的意见。

5 法律风险管理过程

5.1 概述

法律风险的管理是循环提升的，宜嵌入组织的所有活动和业务。5.2～5.5 介绍了法律风险管理过程，如图 2 所示。

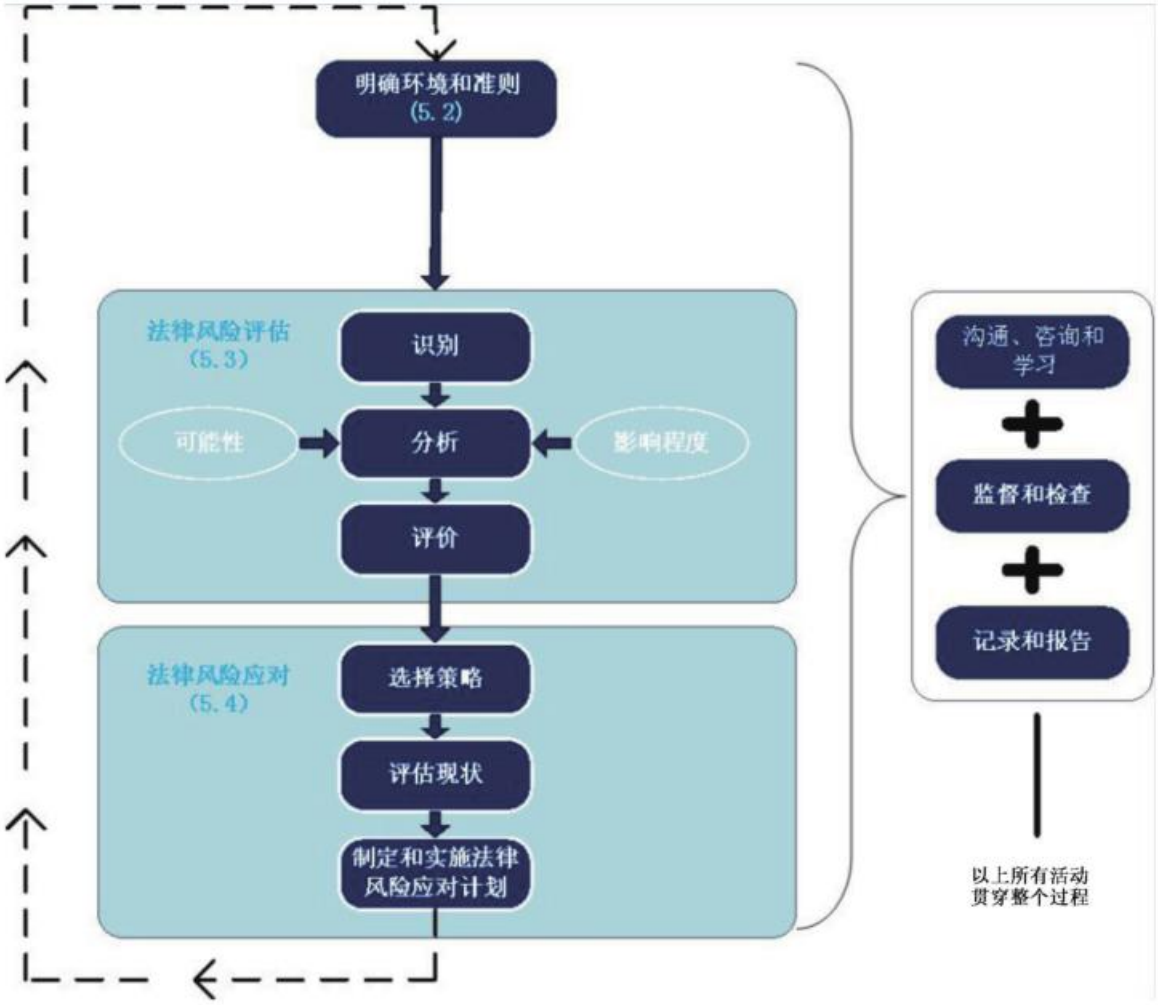

图 2 法律风险管理过程

监督和检查、报告、沟通和协商宜贯穿组织内法律风险管理的全过程。详细介绍请见 5.5。

5.2 明确环境和准则

5.2.1 概述

明确法律风险环境信息是应用适当的方法，对组织内外部环境中与法律风险相关的信息进行收集、分析、整理、归纳的一系列过程。通过明确法律风险环境信息，组织可明确其法律风险管理目标，确定与组织相关的内部和外部参数，并设定法律风险管理的范围和有关风险准则。

5.2.2 法律风险外部环境信息

法律风险的外部环境信息是指处于组织外部但与法律风险管理相关的因素，主要包括：

——相关的本地和国际法律及其变化；

——支持法律风险管理的外部服务提供者和顾问，如律师事务所、外部审计师、管理咨询机构以及信息管理和分析服务的提供者；

——外部利益相关者，如相关的企业、社会组织、监管机构、地方政府、公众、利益团体、新闻媒体等；

——第三方的任何作为或不作为，例如第三方的欺诈和欺骗行为；

——适用的国际协议和谅解备忘录；

——与组织相关的市场条件；

——第三方诉讼或索赔；

——涉及产品/服务的提供、运输、交付所在国的法律。

审查和了解在多个司法管辖区运营的组织的法律风险外部环境时，可考虑不同司法管辖区之间的环境和文化差异。国家法律的域外适用，即特定情况下适用哪个司法管辖区的法律（即冲突法和法律的相互承认），以及相关管辖权的识别可能也需要加以考虑。

5.2.3 法律风险内部环境信息

法律风险的内部环境信息是指组织内部与法律风险及其管理相关的各种信息，主要包括：

——组织的战略目标和治理结构；

——组织的业务模式；

——组织的主要业务及管理流程/活动、部门职能分工等相关信息；

——组织在法律风险管理方面的使命、愿景、价值理念；

——组织法律风险管理工作的目标、职责、相关制度和资源配置情况；

——组织法律事务工作及法律风险管理现状；

——利益相关者的法律遵从情况和激励约束方式；

——组织签订的重大合同及其管理情况；

——组织发生的重大法律纠纷案件或法律风险事件的情况，以及相关的法律规范库和法律风险库；

——组织的财务管理情况；

——组织知识产权管理情况；

——组织法律风险管理的信息化水平；

——与法律风险及其管理相关的其他信息。

5.2.4 确定法律风险准则

法律风险准则是衡量法律风险重要程度所依据的标准，需体现组织对法律风险管理的目标、价值观、资源、偏好和承受度。法律风险准则宜在法律风险管理工作开始实施前制定，并根据实际情况进行相应调整。

法律风险的准则：

——是组织风险准则的一个子项；

——是识别、界定和评估某项或某一组法律风险的重要性和可接受水平的措施；

——反映与法律风险有关的全面风险管理的目标、价值、资源、偏好和容忍程度；

——定期并在任何重大项目开始时进行审查，以更新法律风险管理的准则和程序；

——可源自或产生于法律适用、合同义务或责任；

——是动态的，且一旦界定，属于法律风险管理的职能；

——与组织管理法律风险和/或政策的整体方法相匹配，组织宜根据实际情况制定和调整法律风险准则。

在确定法律风险的准则时，组织需考虑的因素包括：

——组织的目标和优先事项；

——组织治理，包括组织内法律风险管理的权力层级以及责任、角色和职责的分配；

——法律风险管理的政策、议定书、框架、程序和方法的现状；

——为确定法律风险水平等级而适用的原则；

——本组织法律风险管理的范围、目标、对象以及法律风险的分类；

——法律风险事件发生的可能性、影响程度以及法律风险等级的度量方法；

——法律风险等级的划分标准；

——利益相关者对法律风险的接受程度或风险水平的容忍度。

下列情况可能需要适用法律风险的准则：

——法律要求组织承担、遵循或批准的事项；

——法律要求组织采纳的与政策或合同有关的事项，或需要组织依法作出决定；

——与机构责任和合规相关的实质问题，包括政府调查、违法行为的指控、可能牵连组织的犯罪行为、重大不合规行为、引发数据保护和隐私问题的数据丢失、吹哨人投诉、导致声誉损失和其他诉讼的事项；

——关于信息披露、意外事件、违法和任何其他情况；

——“非正常业务”的诉讼与和解，如其所涉金额或呈现的问题涉及上述一项或多项其他因素。

法律风险准则的定义是过程驱动的，要求对法律风险进行分类和量度，以便对其进行量化，并确保使用适当的风险应对方案。

要获得适当的反馈，需要管理层和整个组织内部对法律风险的准则达成一致。过于狭窄的法律风险准则可能会引发意料之外的后果，即将法律风险的持有人与更广泛的经营风险环境分离。这可能产生筒仓效应，即将法律风险管理与风险管理的其他元素隔离。

与组织所采用的全面风险准则不能完全结合的过于限制性的法律风险准则，可能会产生非预期的后果，即对法律风险问题提供的处理方法过于狭隘，负责法律职能的人员只有在危机升级时才会介入而不是在早期阶段介入，而早期介入可能会降低法律风险，且更有能力为法律风险提供应对方案。

5.3 法律风险评估

5.3.1 概述

法律风险评估是法律风险识别、法律风险分析和法律风险评价的整体过程。

5.3.2 法律风险识别

5.3.2.1 概述

识别法律风险的目的是发现和描述能够帮助或阻止组织实现其目标的法律风险。为全面了解法律

风险，组织宜确定法律风险的来源、影响范围、事件（包括环境变化）、原因及其潜在后果。

通过法律风险识别，全面、系统、准确地描述组织各种法律风险的特征，以便明确下一步法律风险分析的目标和范围。在识别法律风险时，需要了解最新的相关信息，如相关背景信息和事实（例如适用法律或市场惯例的变化）。除了识别可能发生的法律风险事件外，还要考虑其可能的原因和可能导致的后果，包括所有重要的原因和后果。不论法律风险事件的风险源是否在组织的控制之下，或其原因是否已知，都要对其进行识别。

组织可选择适合于其目标、能力及其所处环境的法律风险识别工具和技术，参见 GB/T 27921—2023 第 4 章。

5.3.2.2 对法律风险识别有用的信息来源

为保证法律风险识别的全面性、准确性和系统性，组织要根据其规模、复杂性、结构和运营的方式等情况来确定法律风险识别的维度，这些维度包括但不限于以下方面：

——根据组织的目标、工作重点及管理层关注的事项进行识别，通过对上述相关事项的梳理，发现组织重大决策、重大事项、重点工作中可能存在的法律风险；

——根据组织治理、管理、经营、生产等活动识别，即通过对公司治理、集团管控、研发、生产、采购、营销、投资、人力、财务、知识产权、数据、信息系统等活动的梳理，发现每一项治理、生产、经营、管理工作可能存在的法律风险；

——根据组织机构设置识别，即通过对各业务管理职能部门/岗位的业务管理范围和工作职责的梳理，发现各机构内可能存在的法律风险；

——根据利益相关者识别，即通过股东、董事、监事、高级管理人员、一般员工、顾客、供应商、债权人、社区、政府等利益相关者的梳理，发现与每一利益相关者相关的法律风险；

——根据引发法律风险的原因识别，即通过对法律环境、违规、违约、侵权、怠于行使权利、行为不当等引发法律风险原因的识别，发现组织存在的法律风险；

——根据法律风险事件发生后承担的责任梳理，即通过对刑事、行政、民事等法律责任的梳理，发现不同责任下组织存在的法律风险；

——根据法律领域识别，即通过对不同的法律领域（如合同、知识产权、招投标、劳动用工、税务、诉讼仲裁等）的梳理，发现不同领域内存在的法律风险；

——根据法律、法规识别，即通过对与组织相关的法律、法规的梳理，发现不同法律、法规中存在的法律风险；

——根据以往发生的案例识别，即通过对本组织或本行业发生的案例的梳理，发现组织存在的法律风险。

组织可以根据自身的不同需要，选择以上不同的维度或不同维度的组合，进行法律风险识别。

附录 A 给出了从“引发法律风险的原因”和“组织主要经营管理活动”两个角度进行法律风险识别的示例。附录 B 给出了法律风险清单的示例。

5.3.3 法律风险分析

5.3.3.1 概述

法律风险分析是指对识别出的法律风险进行定性或定量分析。分析的结果为法律风险评估和应对提供输入信息。法律风险分析要考虑导致法律风险事件的原因、法律风险事件发生的可能性及其后果、影响后果和可能性的因素等。

分析法律风险事件发生的可能性和影响程度，可以单独使用或组合使用历史数据模拟、商业分析、人工智能和建模以及专家意见，请参阅 GB/T 27921—2023 了解更多关于风险分析技术的信息。也要

考虑模型和专家意见本身的局限性。

法律风险与其他风险在一定条件下具有伴生性和相互转化性，组织要对法律风险与其他风险之间的关联性进行分析，明确各风险事件之间的影响路径和传递关系，明确法律风险与其他风险之间的组合效应，从而在风险应对策略上对法律风险和其他相关风险进行统一集中的管理。

5.3.3.2 法律风险可能性分析

对法律风险发生可能性进行分析时，可考虑但不限于以下因素：

——法律、法规的完善程度及有关机构的执法、司法措施及惯例的状况；

——改进和遵守现有的法律风险管理框架，包括战略、管理、内部规则和政策；

——利益相关者对法律、组织的规则和政策的实际遵守情况；

——在一定期间内发生的与法律风险有关的活动的频率和数量；

——对以往法律风险事件进行记录、分析和吸取教训；

——所涉及工作的频次，即与法律风险相关的工作在一定周期内发生的次数。

附录C给出了供参考的法律风险发生可能性分析的示例。

5.3.3.3 法律风险影响程度分析

对法律风险影响程度进行分析时，可考虑但不限于以下因素：

——后果的类型，包括财产类的损失和非财产类的损失等；

——后果的严重程度，包括财产损失金额的大小、非财产损失的影响范围、利益相关者的反应等。

附录D给出了供参考的法律风险影响程度分析的示例。附录E给出了供参考的在审查合同时需要关注的关键条款和意见。

5.3.4 法律风险评价

法律风险评价是指将法律风险分析的结果与组织的法律风险准则相比较，或在各种风险的分析结果之间进行比较，确定法律风险等级，以帮助组织做出法律风险应对的决策。组织的决策需考虑：

——更广泛的组织环境，包括内部和外部利益相关者的观点；

——组织的目标、优先事项和风险管理政策；

——组织和利益相关者的价值观、道德和伦理；

——组织的风险态度和风险容忍度；

——组织的风险概况(包括组织在法律风险管理方面的成熟度及其在商业活动中的地位)。

在可能和适当的情况下，可采取以下步骤进行法律风险评价：

——在法律风险分析的基础上，对法律风险进行不同维度的排序，包括法律风险事件发生可能性的高低、影响程度的大小以及风险水平的高低，以明确各法律风险对组织的影响程度；

——在法律风险水平排序的基础上，对照组织法律风险准则，可以对法律风险进行分级，具体等级划分的层次可以根据组织管理的需要设定；

——在法律风险排序和分级的基础上，组织可以根据其管理需要，进一步确定需要重点关注和优先应对的法律风险。

5.4 法律风险应对

5.4.1 概述

法律风险应对是指组织针对法律风险或法律风险事件所采取的相应措施，将法律风险控制在企业可承受范围内。风险评估是制定风险应对计划的先决条件，并使组织能够就法律风险应对方案作出明

智的决定。组织评估其法律风险时，要证明该等风险得到恰当管理，否则组织可能会面临不利的诉讼和损失。

法律风险应对包括选择法律风险应对策略、评估法律风险应对现状、制定和实施法律风险应对计划三个环节。风险应对策略宜考虑一系列应对方案，其中可能包括法律补救措施，也包括财务、运营和声誉补救措施。

5.4.2 选择法律风险应对策略

法律风险应对策略包括规避风险、降低风险、转移风险、接受风险和其他策略等，可将其单独或组合使用。在选择适当的法律风险应对方案时，宜考虑以下因素：

——组织的战略目标、核心价值观和社会责任等；

——组织对法律风险管理的目标、价值观、资源、偏好和承受度等；

——法律风险应对策略的实施成本与预期收益；

——利益相关者的诉求和价值观、对法律风险的认知和承受度以及对某些法律风险应对策略的偏好；

——管理风险所需资源的可获得性和分配情况；

——法律允许的法律风险可转让、转移或投保的范围；

——组织内风险意识和成熟度水平。

关键风险指标(KRI)为特定风险应对方案能否有效管理法律风险提供一定指导。为选择有效的KRIs，组织可识别由其操作过程生成的潜在数据。KRI可按单个指标(例如“合同价值”)的形式进行报告，但它们与相关数据结合时，通常可以提供更优的信息。以下是部分KRI组合的示例：

——合同责任与合同价值：可按合同类型、合同相对方、第三方等维度分类，可分析合同责任与价值，以评估组织为赢得特定业务领域所承担的风险；

——未签合同事实履行情况：通过分析书面合同签署量与实际交易量情况，可分析组织是否在未签署有约束力的书面合同的情况下开展交易；

——法律合规培训：如通过查看分析销售人员的产品销售与合规培训登记情况，可分析组织针对客户注意义务可能发生的行为风险。如果组织的销售团队没有完成他们的合规培训，或者经常很迟才完成，他们可能没有认识到法律监管合规方面的最新问题，并因此导致其所在组织暴露在不断增加的法律风险中。

5.4.3 评估法律风险应对现状

组织选择法律风险的应对方案时，要对组织的法律风险应对现状予以评估，以了解目前的法律风险应对存在哪些不足和缺陷，为制定法律风险应对计划提供支撑。

评估法律风险应对现状至少要考虑以下几方面的因素：

——资源配置，即组织内部的相关机构设置、人员、设备和经费配备能否满足法律风险应对需要；

——职责权限，即是否明确与风险应对相关的职责和权限；

——过程监控，即是否要求对持续性业务管理活动进行定期或不定期的监督和控制、证据资料保留、信息沟通和预警；

——奖惩机制，即对相关人员在法律风险应对工作中的绩效是否设立了奖惩机制；

——执行者能力要求，即对与法律风险应对相关的内部执行者是否有明确的资质、能力要求；

——部门内法律审查，即是否要求业务部门内部对一般性的法律问题进行审查；

——专业法律审查，即是否要求法律部门或专业律师对专业性法律问题进行审查或提供相关法律意见；

——法律风险意识，即相关人员对法律风险的存在、可能造成的后果，以及如何开展法律风险应对

等方面是否有必要的认识和理解。

5.4.4 制定和实施法律风险应对计划

在选择和实施适当的法律风险应对方案后，组织需评估其是否能够接受剩余风险（可能不一定是法律风险，而是其他风险）。如果剩余风险是不可接受的，组织宜调整或制定新的风险应对方案，并在考虑这种调整及其影响后重新评估风险，直到剩余风险处于可接受的水平。

在实施法律风险应对计划时，组织需考虑 GB/T 24353—2022 的 6.5.3 和以下内容。

——政策和程序：制定或改进与法律风险应对有关的政策和程序。例如，当法律纠纷发生或可能发生时，明确要求内部利益相关者通知内部或外部律师。

——标准操作规范（SOPs）：为内部利益相关者制定标准操作规范。例如，制定内部利益相关者需向第三方披露业务信息时所适用的标准操作规范，辅以经批准的不披露或保密协议，以避免保密信息的意外披露。

——技术和科技：使用技术应对部分法律风险。例如，使用合同评审模板来确保合同的关键法律风险在合同签署之前得到识别和处理，或者开发或提升信息安全以避免未经授权访问组织的信息系统而产生的法律风险。

——信息：提升法律风险管理所需信息的可获得性。例如，通知合同缔约方，除非在指定的时间范围内通知对方，合同将自动续期，或者发布关于法律风险引发的某些事件的风险预警信息。

——活动：开展法律风险应对活动。例如，由法律专家进行合同审查和重新起草，或选择合适的争议解决方法（诉讼、仲裁或调解）、争议解决专家和适当的争议解决策略。

——培训和示例讲解：为主要的内部利益相关者提供法律风险管理方面的培训，以提高他们的技能和法律风险意识。例如，培训课程概括了相关法律、此类法律对个人在工作中角色的影响，以及违规对个人的后果。

法律风险管理是一个动态、循环往复的过程，所使用的技术需要根据内部和外部法律风险环境的变化进行评估和调整，以确保其有效性。

组织需跟踪和监控法律风险应对的效果和外部环境，评估不断变化的风险，并在必要时重新制定法律风险应对方案。法律风险应对措施通常包括以下几种类型：

——资源配置类，指设立或调整与法律风险应对相关的机构、人员，补充经费或风险准备金等；

——制度、流程类，指制定或完善与法律风险应对相关的制度、流程；

——标准、规范类，指针对特定法律风险，编写标准、规范等文件，供相关人员使用；

——技术手段类，指利用技术手段规避、降低或转移某些法律风险；

——信息类，指针对某些法律风险事件发布预警信息；

——活动类，指开展某些专项活动，规避、降低或转移某些法律风险；

——培训类，指对某些关键岗位人员进行法律风险培训，提高其法律风险意识和法律风险管理技能。

在法律风险应对措施确定之后，可制定应对措施的实施计划。实施计划中至少包括以下信息：

——实施法律风险应对措施的机构、人员安排，明确责任分配和奖惩机制；

——应对措施涉及的具体业务及管理活动；

——报告和监督、检查的要求；

——资源需求和配置方案；

——实施法律风险应对措施的优先次序和条件；

——实施时间表。

在制定法律风险应对措施后需评估其剩余风险是否可以承受。如果不可承受，宜调整或制定新的法律风险应对措施，并评估新的措施的效果，直到剩余风险可以承受。

实施法律风险应对措施会引起组织风险情况的改变，需要跟踪、监督有关风险应对的效果和组织的环境信息，并对变化的风险进行评估，必要时重新制定法律风险应对措施。法律风险应对是一个递进的动态过程，需要根据内外部法律风险环境变化对制定的措施进行评估调整，以确保措施的有效性。

5.5 法律风险管理的沟通（内部和外部）、咨询和报告机制

5.5.1 概述

组织需建立：

——GB/T 24353—2022 的 6.2 所述的内部沟通和报告机制，以确保在适当的时间和层级对其法律风险管理系统的关键内容进行适当的沟通；

——将沟通机制和途径与其他风险信息来源关联，以确保组织内部以及与外部利益相关者之间顺畅沟通。

外部沟通和报告需确保维持保密、法律职业特权和关于律师和客户的保密特权（或相关司法管辖区的同等形式保护措施）的要求。

5.5.2 沟通、咨询和学习

组织需在法律风险管理过程的各阶段与有关利益相关者进行及时沟通和咨询，以确保这些利益相关者（包括实施法律风险管理的内部人员）充分理解法律风险及其对组织的影响。有关利益相关者还可了解其在法律风险管理决策过程中的作用，并能够根据相关信息做出适当决策。

由于组织的各级人员以及外部利益相关者具有不同的价值观、观点和关注点，他们对法律风险管理的偏好和期望也可能不同。这对法律风险管理的决策和实施具有重要的影响。因此，在决策过程和风险应对方案实施过程中，与有关利益相关者的沟通和协商可包括建立健全监测和审查流程，并保存风险管理实践的记录（详见 5.5.3）。为促进有效的沟通和协商，组织宜致力于向每个负有管理法律风险的责任、职责和权力的人员提供必要的信息。管理职能机构还需与有关利益相关者沟通，包括监管机构、立法和司法机构以及其他外部利益相关者。

为在整个组织内建立风险管理文化，学习活动可：

——在法律风险管理的所有阶段进行；

——提高对法律风险的认识和理解；

——用于更清晰地理解关于治理和领导、授权、目的和目标、利益相关者的参与、角色和职责，以及政策、过程和程序的一致性。

5.5.3 监督和检查

对法律风险管理的监督和检查包括以下内容：

——随时了解环境的变化，例如引入新的法律和执行这些法律，以便调整组织的相应战略；

——监督法律风险引发的事件，分析其频率和模式，并从中得出结论（包括与其他风险的潜在相关性和对其他风险的放大效应）；

——考虑与主要利益相关者建立预警系统，以识别可能出现的重大法律风险的预警信号；

——监督和检查的具体内容包括：

- 风险应对的结果，
- 环境的变化，
- 制定综合风险应对计划，
- 指定责任和义务方；

——与风险应对计划进展进行比较，定期及适时地审查及更新风险应对计划，以确保其在法律风险

管理方面的充分性、适宜性及有效性。

5.5.4 记录和报告

组织宜考虑与记录、保存和报告有关的下列事项：

——法律职业特权，关于律师和客户的保密特权和工作成果（或相关国家法律下的同等概念和术语）；

——根据数据保护法制定的销毁、保留和隐私政策；

——利益相关者为改进决策和内部或外部审计目的而获得和获取文件；

——是否需要妥善保存相关文件，并通过一系列证明性程序来证明相关文件、资料或证据并无更改；

——与机密性文件有关的保密和安全措施，例如对此类文件设置有限和需授权的访问程序。

组织需报告在实施法律风险管理和遵守措施方面的变化情况。

6 法律风险管理的实施

6.1 概述

法律风险管理需嵌入组织的活动和运营中，确保其结果是组织决策过程的一部分。法律风险管理的实施宜与组织的战略、组织内部的风险管理框架、目标和管理制度相结合，包括法律风险管理的方针、组织职能、资源配置、信息沟通机制等。

6.2 法律风险管理方针

法律风险管理方针需明确下列事项：

——组织法律风险管理理念；

——最高管理者对法律风险管理的承诺；

——组织法律风险管理的目标；

——组织的法律风险偏好；

——组织法律风险管理目标与组织的目标及其他风险管理目标的关系；

——组织法律风险管理目标的层次分解和细化；

——持续改进的承诺。

6.3 法律风险管理的组织机构及职能

组织可设立专门的法律风险管理机构或者岗位，并明确其职责和内容，具体包括但不限于：

——明确本组织法律风险管理机构或岗位的人员组成，根据组织内部条件和管理需求，必要时可设置总法律顾问，从总体上负责组织的法律风险管理工作；

——明确内外部法律风险管理资源的分工和合作方式；

——明确法律风险管理体系的制定、实施和维护人员的职责；

——明确执行法律风险应对措施、维护法律风险管理体系和报告相关风险信息人员的职责；

——明确管理人员及其他员工在其本职工作中有关法律风险管理方面的职责；

——建立批准、授权制度；

——建立考核方法、奖惩制度。

6.4 法律风险管理的制度流程

组织可根据其法律风险管理的目标，建立完善适当的配套制度和行为规范，确定法律风险管理的工

作程序，同时结合组织内部控制管理工作，将法律风险纳入到流程控制中，确保法律风险管理工作切实融入组织的日常管理工作中，确保法律风险管理在组织内部的统一理解和执行。具体要考虑：

——本组织法律风险管理工作的范围和内容；

——法律风险管理制度、规范的制定要考虑组织的制度体系，特别是风险管理制度，确保一致性；

——形成对制度规范的定期更新，确保时效性。

6.5 法律风险管理的资源配置

组织需根据法律风险管理计划，制定可行的方法，为法律风险管理分配适当的资源。具体要考虑：

——法律风险管理相关人员的技术、经验和能力要求；

——法律风险管理过程每一阶段所需要的资金及其他资源；

——法律风险管理目标、成本和收益的关系。

此外，组织可根据内部条件和管理需求，通过建立法律风险管理信息系统，完成法律风险环境信息的收集，法律风险识别、分析、评价，应对，监督与检查，沟通和记录等各项工作，实现法律风险信息的在线查询、检索和维护，支持法律风险管理的动态管理。

6.6 法律风险管理意识

组织宜考虑下列因素，促进法律风险管理意识的提高：

——最高管理层对法律风险管理的态度、管理理念和承诺；

——提高重要流程及核心岗位员工法律风险管理的意识和能力；

——系统的法律风险管理培训方案，包括相关专业的专家提供的研习会、课程和培训；

——为本组织成员以及多学科工作组的意见建立沟通渠道，以改善法律风险管理；

——加强对内部违法违规行为的惩治力度，形成良好的法律风险管理文化。

附 录 A
（资料性）
法律风险识别方法示例

法律风险管理需要一种结构化的方法来评估组织面临的法律风险。通过采用适当的风险管理技术，组织可主动识别法律风险，以减少、消除风险，或重新配置其流程以最大程度降低法律风险敞口。

法律风险识别矩阵（LRIM）是按照业务领域/单位/活动将识别和梳理的法律风险归入不同类别的一种方法。通过考虑各种相关的业务领域/单位/活动，LRIM 将各种类型的法律风险与组织运营联系起来。在一个 LRIM 中，所有已识别的法律风险事件都被归入不同的类型中。这些不同类型的法律风险可能发生在不同的业务领域，有不同的原因和特点。LRIM 有助于系统地理解组织的所有法律风险。表 A.1 提供了一个从“引发法律风险的原因”和“组织主要经营管理活动”两个角度进行法律风险识别的示例，该示例将法律风险分为六种不同类型，并对各类型进行了简要说明。

为使法律风险的分类有用，重要的是要认识到每个类别可能不是相互排斥的，单项商业活动可能产生属于一个或多个类别的法律风险。

表 A.1 法律风险识别方法示例

参数	类型 1	类型 2	类型 3	类型 4	类型 5	类型 6
法律风险类型	法律环境	违规行为	违约行为	侵权行为	怠于行使权利	不当行为
活动 1						
活动 2						
活动 3						
……						

关键提示

类型 1：如组织在其运营的环境、市场或区域中面临重大法律变更，或者组织决定进入新的环境、市场或区域且组织对该环境、市场或区域的法律不熟悉或者当地法律在某些方面可能存在缺失，则可能会导致法律风险环境的不可预测性。

类型 2：违规行为是指组织违反适用法律。例如，组织在履行其对监管者的财务报告义务时，未做出适当的披露。

类型 3：违约行为是指组织或合同相对方不履行或不当履行合同义务并引发法律后果，如损害赔偿请求权或守约方因违约而终止合同的权利。例如，组织未能根据其合同义务按时交付货物。

类型 4：组织侵犯、违反或触犯第三方的合法权利或预期，则可能构成侵权行为。例如，未经许可使用第三方的商标会侵犯第三方的知识产权。侵权行为可能产生于合同一方的合同义务，也可能在没有合同义务的情况下发生。

类型 5：如行为未达到法律规定的保护他人不受不合理损害的行为标准，则可能发生怠于行使权利的情况。组织可能会疏忽行事，也可能成为他人疏忽的受害者。此外，组织在行使自身的权利、义务和责任时可能会因疏忽大意，造成对组织的损害。例如，如果组织没有及时通知它的保险公司它所遭受的损失，这种行使权利的疏忽可能导致损失无法被组织与保险公司的合同覆盖。

类型 6：当组织就一个法律风险问题有若干可采取的行动时，就可能出现不当选择。所有这些行动都可能是合法的，但每一项行动都有不同的成本、影响和后果，即一个或多个替代选项在决定做出时被放弃。例如，公司可以选择尝试通过诉讼或仲裁解决与贸易伙伴的争议。任何一种方式——诉讼或仲裁，都可以解决争议，但每种方式在维护当事人之间的商业关系、在行业和社区中的声誉、投入的时间和产生的成本方面都有不同的影响。

附 录 B
（资料性）
法律风险清单示例

法律风险清单是对可能发生的法律风险事件的汇总，包括相应的法律、可能的结果和影响程度。它帮助使用者识别与相关法律有关的法律风险。具体示例见表 B.1。

表 B.1 法律风险清单示例

经营活动	法律风险类型	识别的法律风险事件（日期、发生情况）	相关适用法律	法律后果	既往案例	内部法律团队的意见	外部法律顾问的意见	建议的方案/行动计划

组织编制法律风险清单宜在其内部法律部门和/或外部法律顾问的指导和监督下开展，以确保法律风险清单在其司法管辖区仍受到相关法律职业特权的保护。表 B.2 给出了具体示例。

表 B.2 获取的法律意见、定量/定性的分析和决策

内部法律团队的意见	外部法律顾问的意见	法律风险问题定量分析	法律风险问题定性分析	向组织董事会或负责团队推荐的应对方案	董事会或负责团队的决策

组织需定期审查其法律风险清单。作为审查的一部分，可以制定一套结构化的访谈问题，以征求业务和运营团队负责人的意见，并审查控制环境的风险敞口和有效性。这些问题可与最近一次审查相匹配，并宜纳入组织自最近一次审查后的变化情况。表 B.3 给出了结构化访谈问题的示例。访谈的方法，可以对过去进行反思，并探索与业务和运营团队合作以支持其法律风险管理的新方法。部分法律风险并不总是会升级到组织的董事会层面，而是由负责团队（即组织中拥有必要权力的人员）考虑根据推荐的应对计划做出决策。

表 B.3 结构化访谈问题示例

访谈问题	提问目的
风险控制如何影响关于法律风险管理的决策	高级经理考虑法律风险管理过程的稳健程度如何？信息交流情况如何？他们使用什么信息来实现监控
您有多少份合同包含会生效的自动续期条款	受访者是否对其现有合同具有良好的认识，并对其进行积极管理
您所在的组织在特定期间订立了多少份合同	是否具备合同管理流程
您所在的组织谈判了多少交易？交易签署的内容与标准条款和条件有哪些偏差	对谈判活动的管理目前处于什么水平
与组织发生争议的最大原因是什么	任何潜在问题领域，以及对诉讼问题是否具有普遍认识

附 录 C
（资料性）
法律风险发生可能性分析示例

法律风险相关事件的发生可能性是指在组织目前的管理水平下，法律风险相关事件发生概率的大小或者发生的频繁程度。对法律风险发生可能性的量化分析，可以从以下 5 个维度进行，每个维度可以进一步细化为若干评分标准，以下示例影响程度分为 5 个等级，分别赋予 1 分至 5 分，表示发生可能性依次加强，得分越高意味着风险发生的可能性越大。对照该评分标准，同时根据不同维度对风险发生可能性影响程度的不同，为各维度设定权重系数，并确定计算公式，最终即可计算出该风险发生可能性的得分。具体如表 C.1 所示。

表 C.1 法律风险发生可能性分析示例

分析维度	1	2	3	4	5
内控制度的完善与执行	内部控制规章制度/业务流程很完善，内部控制规章制度/业务流程执行非常准确	内部控制规章制度/业务流程很完善，内部控制规章制度/业务流程执行比较准确	内部控制规章制度/业务流程较完善，内部控制规章制度/业务流程执行程度一般	内部控制规章制度/业务流程较完善，内部控制规章制度/业务流程较难得到执行	内部控制规章制度/业务流程很不完善，内部控制规章制度/业务流程很难得到执行
我方人员相关法律素质	非常熟悉相关法律及组织内部制度并能够完全有效执行	理解相关法律及组织内部制度，并能够较好执行	了解相关法律及组织内部制度，且基本能够执行	对相关法律及组织内部制度有一定了解，但不能有效执行	不了解相关法律及组织内部制度
相对方风险状况	履约能力很强或侵权可能性很小，信誉很好	履约能力较强或侵权可能性较小，信誉较好	履约能力一般或侵权可能性一般，信誉一般	履约能力较弱或侵权可能性较大	履约能力很弱或侵权可能性很大，信誉很差
外部监管执行力度	有法律规定，有监管部门，违法行为总是能得到及时查处，且处罚严厉	有法律规定，有监管部门，违法行为一般都能得到及时查处	有法律规定，有监管部门，但违法行为并未都得到及时查处	有法律规定，有监管部门，但监管部门经常不履行职责	无法律规定，有监管部门，但监管部门经常不履行职责
工作频次	风险行为所涉及的工作每年至少发生一次	风险行为所涉及的工作每季度至少发生一次	风险行为所涉及的工作每月至少发生一次	风险行为所涉及的工作每周至少发生一次	风险行为所涉及的工作每天至少发生一次

附 录 D
（资料性）
法律风险影响程度分析示例

法律风险事件的影响程度是指该风险事件会对组织的经营管理和业务发展所产生影响的大小。对法律风险影响程度的量化分析，可以从以下 3 个维度进行，每个维度可以进一步细化为若干评分标准，以下示例影响程度分为 5 个等级，分别赋予 1 分至 5 分，表示影响程度依次加强，得分越高意味着风险影响程度越大。对照该评分标准，同时根据不同维度与风险影响程度相关性的不同，为各维度设定权重系数，并确定计算公式，最终即可计算出该风险影响程度的得分。具体如表 D.1 所示。

表 D.1 法律风险影响程度分析示例

分析维度	1	2	3	4	5
财产损失大小	10 万元以下	10 万元～100 万元	100 万元～500 万元	500 万元～5 000 万元	5 000 万元以上
非财产损失大小	商誉、组织形象、知识产权等损失很小	商誉、组织形象、知识产权等损失较小	商誉、组织形象、知识产权等损失一般	商誉、组织形象、知识产权等损失较大	商誉、组织形象、知识产权等损失很大
影响范围	很小范围的区域，如组织内部	较小范围的区域，如若干组织间	中等范围的区域，如全市范围内	较大范围的区域，如全省范围内	很大范围的区域，如全国范围内
注：经济损失的区间界定将根据组织的规模、组织的性质、组织运营活动所在的国家，以及组织在不同货币区域运营时的货币价值和波动而有所不同。					

附 录 E
（资料性）
审查合同需关注的关键条款

本附录简要总结了审查合同时，为最大限度降低法律风险所关注的关键条款。以下事项清单并不旨在替代法律咨询意见，也不是要提供一个包含所有合同事项的全面清单。这些事项中的大多数本质上是商业事项，需要商业决策，但鉴于它们被嵌入了合同，或须在合同中处理，在此意义上它们构成“法律风险”。

组织可检查表 E.1 中列出的所有事项是否已被合同覆盖，或至少已取得关注（即使这些事项被撤销）。为产品、服务或成本收益而接受更大的风险可能是合适的。组织可视其是否为以下角色，从相关角度审议每一事项：

a） 货物的供应商或服务的提供者；

b） 货物的购买者或接受服务的客户。

表 E.1 审查合同需关注的关键条款示例

事项	注意问题
缔约资格	核查相对方是否具有签订具有法律约束力协议的法律资格
对价	对于需要对价才能达成有约束力的法律协议的司法管辖区，检查是否存在有效的对价
交货/装运条件	买方是否需要在特定日期取得货物（可能是为履行与第三方的合同义务）？如果是这样，宜起草交货条款以确保： ——时间是交货的关键； ——买方因此遭受的任何实际损失可得到补偿。 卖方宜注意以下情况：a）条款中规定的损失是否未设上限；或 b）买方指定的交货日期是否存在无法满足的高风险
法定所有权转移	在货物合同下，法定所有权何时转移至买方（即何时成为买方的财产而非卖方的财产）？ 如果所有权在交付日期前转移，且组织正在购买货物，则组织宜确保从该日期起对货物进行保险。如未能取得保险，则组织控制货物前，存在因货物损坏或破坏引发经济损失的风险
撤销（货物合同）	组织作为买方，需要取得撤销订单的权利吗？ 组织作为卖方，宜设法将买方撤销其订单的时间限制在法定限度内，否则，其可能会因在订单取消日前服务于订单的时间而蒙受损失
服务的中止和终止（服务合同）	合同是否赋予服务提供者在某些事件或条件下暂停服务或完全终止服务的权利？这些约定理论上并非不合理，但它们宜： ——只限于真正重要的事项； ——为客户提供一种选择，以纠正被指控的违约行为或某种形式的冲突升级，而非立即执行（除非发生真正的紧急情况）； ——给予客户足够时间，使其就数据或服务作出其他安排。 客户组织也可就以下事项获得保证：至少在终止后的特定期限（或为“商业合理”期限，如果服务提供者不愿意承诺具体期限），数据可继续以可使用的格式获取，以及服务提供者在合同解除时将返回或者销毁客户的任何数据副本

表 E.1　审查合同需关注的关键条款示例（续）

事项	注意问题
付款	付款条件是什么？是指发票的日期或交货日期，还是指客户收到发票的日期？ 逾期付款有利息吗？是否存在对付款提出异议的权利？ 是否明文约定对于付款而言“时间是至关重要的”（在这种情况下，逾期付款可能使卖方有权终止合同）
违约赔偿/责任	违约赔偿： 组织可考虑其希望从另一方获得什么形式的违约赔偿。 组织宜寻求直接损失的赔偿，但其宜同时寻求间接或从属损失的赔偿吗？如果供应商接受间接或从属损失，这些损失可能会很广泛，并可能使其责任超出合同价值。 责任限制： 组织需考虑是否可以接受对另一方不履行合同义务的责任的任何限制。 如果另一方希望将组织的责任限制在高于组织为该等责任所投保的数额，组织宜对其予以关注
分批装运、分批交货和分批数量	分批装运和交货是否能被接受？ 如果分批交货或分批装运，则组织面临另一方在全部订单交付前破产或停止贸易的风险
退货	在什么情况下买方可以退货？ 如果组织已经购买了货物，并且供应商坚持在非常局限的条件下接受退货，那么组织就可能面临购买价格支付后没有按照预期的标准收到货物的风险。在这种情况下，组织将需要决定是接受货物还是向另一方付款采购符合其最初期望标准的货物。 组织在销售货物时，宜设法限制退货的期限。否则，组织将面临买方在货物很可能失去价值后退回货物的风险。 另一种选择是争取在购买前对货物进行测试或检查的权利
保密	合同是否充分禁止相对方泄露组织希望保密的信息，例如商业秘密甚至是协议存在的事实？ 供应商通常希望公布其过往交易以吸引更多的业务（有时使用客户的徽标或商标），但如果供应商接触客户组织的竞争对手并公开客户组织签订合同的条款，这对客户组织来说是一个风险。 保密条款可包含在合同中，以便： ——宽泛地界定保密信息的含义（包括所有数据、非书面信息以及对方可接触到的任何文件的内容）； ——对允许披露的情形进行限制（例如监管或刑事调查，或法律允许的披露）
破产	另一方有可能在履行合同规定的全部义务之前破产。其破产将对合同造成什么影响？ 如果组织认为另一方存在不履行其合同义务的风险，组织可以主张将担保人纳入合同（通常是母公司），以担保履约
保证事项的免责	作出了哪些保证和免责声明？合同是否放弃了所有的重要保证？如果是，考虑这是否与当地法律不一致，因为部分保证作为法律事项（例如，受法定保护）不能被放弃。合同至少宜保证服务符合其要求（要求尽可能详细，以避免误解和分歧）并按照该等要求执行，且服务不侵犯任何第三方的知识产权，否则客户组织可能面临不受合同约定的任何责任限额限制的第三方索赔的风险。 如果没有这两项保证，就很难确保服务实际上会按照服务提供者的营销人员声称的方式开展，或服务提供商有权向客户提供服务

表 E.1　审查合同需关注的关键条款示例（续）

事项	注意问题
适用法律和管辖权	合同最有可能规定其受卖方/服务提供者所在国的法律管辖，并授予该国法院对因本合同引起的任何争议的专属管辖权。 作为客户的组织，面临相对方国家的法律无法提供足够法律救济的风险。 组织可以考虑的一些选择包括： ——明确组织所在司法管辖区的法律和管辖权（大型服务提供商可能在所有相关区域内开展业务并受其管辖，因此对它们而言无重大不便）； ——规定争议必须在被告所在司法管辖区内提出（该方法具有公平性，倾向于鼓励以非官方途径解决争议，因为索赔人不享有“本国法院”的优势）； ——删除该条款，将问题留待以后需要时讨论和解决。但是，这种办法将受到国际公法的制约，这可能对组织不利。 组织面临的另一个风险是，由于所选司法管辖区的法院（缺乏）管辖权，其可能面临所缔结的合同最终不可执行的风险
赔偿	赔偿的目的是在风险不在当事人控制范围内时，限制一方所面临的风险。但是，赔偿的范围如果没有适当的限制，可能会进一步引发风险。组织可以主张赔偿： ——只适用于某些损失（参见违约赔偿部分）； ——规定赔偿金额的上限。 组织是否不仅要就自身行为（不一定是不合理的），还要就其承包商或其他第三方（组织可能在其他情况下不对这些人承担替代责任）的行为，对相对方进行赔偿？建议不要自愿承担这种责任。如果组织接受赔偿安排，则需要仔细考虑赔偿的范围，例如，它是一种无限赔偿吗？ 大多数供应商/服务提供者的标准合同不太可能包括任何形式的使客户受益的赔偿。但是，这种保护至少在两个关键领域是重要的，这两个领域大部分（如果不是全部）都在服务提供者的单独控制之下，而且这两个领域的保护和救济费用都可能极高： ——侵犯第三方知识产权； ——披露不当或数据外泄
转让和分包	各方是否能够转让合同的利益或对其合同义务进行分包？ 组织宜考虑其是否要明确限制全部转让权利，以便转让事宜受限于其书面同意。 如果另一方能够将其在合同项下的义务对外分包，则存在分包商可能无法按照与原缔约方相同的标准履行其义务的风险
不可抗力	在相对方控制范围内的事件是否被约定为不可抗力事件，并排除其不履行部分或全部合同义务的责任？ 组织宜考虑哪些因素超出了其控制范围，并试图将这些因素作为不可抗力因素包括在合同中
争议解决	如发生争议，可如何解决？解决争议的方法有很多种，包括诉讼、仲裁、调解等。每项争议解决程序都有其自身的风险，组织宜考虑： ——提出索赔申请的时限或最低金额限度； ——由指定专家解决争议； ——对争议解决程序的结果提出质疑的程序

表 E.1　审查合同需关注的关键条款示例（续）

事项	注意问题
第三方权利	组织所在集团中一名成员签订合同时，第三方权利是否可被排除？ 通常情况下，第三方权利被排除在合同之外。但是，为允许第三方强制执行合同，有时明确包含第三方权利是适当的。例如，集团公司的一个成员为了整个集团的利益而签订合同。 如果第三方权利未被明确限于特定方或特定权利，就会产生风险。为了减少风险，宜明确的措辞包括： ——对第三方进行限制（例如，限制为该方的集团公司）； ——可由任何第三方强制执行的合同权利； ——根据需要，确保第三方权利不会只利于合同一方所在的集团
自动续期	是否存在除非客户事先书面通知、合同自动续期一段时间的约定？ 客户宜设置一个内部流程，以在其需作出关于续期的决定以及发出任何终止通知时作出提示。理想的情况是，合同自动续期（这样客户就不必每次都重新谈判），但也允许经一段较短的合理期限的通知终止合同
合同的变更	相对方是否有权单方面变更其义务？例如，服务提供者有时会试图在未取得客户组织的任何意见的情况下变更其服务。虽然在某些情况下某种形式的变更权利是必要的和适当的（例如更新），但从客户的角度来看，这种方式是有风险的，并且不能向客户保证任何此类变更都是有益的，更不用说是可以接受的了。 较好的做法是限制相对方作出“商业合理变更”的权利。更为妥当的做法是在此基础上增加一项禁止进行“实质性不利”变更的限制
数据保护/隐私	在部分商业合同中，服务提供者将获得组织的数据，这些数据就数据保护和隐私法而言，将构成“个人数据”或“个人可识别信息”（或当地法律下同等含义的术语）。因此，需要在与服务提供者的合同中包含适当的合同条款
数据的位置	部分合同明确保留在其业务所在国存储客户数据的权利。其他合同可能不触及该事项，但服务提供者可能根据（通常是合法的）法无明文禁止即合法的理论，遵循类似的做法。宜考虑将任何个人数据传输到特定司法管辖区以外对数据保护的影响
数据的所有权	当合同要求传输或创建数据时，合同宜明确哪一方是数据所有人的问题。作为数据的提供者，组织宜明确表示所有数据都属于它，服务提供者对这些数据不享有任何权利或许可。还可以明确另一方不取得且不得主张客户数据的任何担保权益
保险	供应商/服务提供者在合同中承诺维持何种保险（例如产品责任、专业赔偿）？ 该等保险的承保范围是什么？ 该等保险的除外责任是什么？ 保险要求是否适用于分包商
索赔时效	索赔通知或提起诉讼是否存在时效限制（这些限制会缩短常规的法定合同索赔时效）？ 如存在时效限制，该期限是从当事人需知道索赔事项或者索赔事项首次发生时起算吗

表 E.1　审查合同需关注的关键条款示例（续）

事项	注意问题
伦理问题	处理相关伦理问题的条款宜包含在供应合同或预期发生供应关系的合同中。这些伦理问题包括反对奴隶制、贩卖人口、有辱人格的工作条件、可持续和公平的商业活动以及本地社区的发展。 最适合使用处理伦理问题的条款的情形是，相对方处于已知此类伦理问题普遍存在或需要积极处理的某一行业，或位于已知此类伦理问题普遍存在或需要积极处理的地点。 这些条款可争取确保处于组织供应链中的实体认同应对伦理道德问题的各项政策。它们还可以包含可选的保证和赔偿条款、国别专用条款、报告义务、审计义务和分包限制。在对特定交易相关供应链中此类伦理问题的风险进行评估之后，可适当地将这些内容包括在内
遵守相对方的政策	相对方可要求组织遵守其政策，如使用条款政策、反贿赂和反腐败政策、数据保护政策等。 相对方极有可能保留随时单方面修改此类政策的权利。同意这样的立场会增加运营成本并引发合规问题。为管理这类条款引发的风险，组织宜考虑： ——要求获取该政策的副本以审查条款； ——要求在该政策与本合同的条款和条件发生矛盾或不一致时，以本合同的条款和条件为准； ——要求相对方在政策发生任何变更前通知组织，以便在这些变更生效之前决定是否继续保持合同关系（并在合同中纳入该等终止权利）

参 考 文 献

[1] GB/T 27921—2023 风险管理 风险评估技术
[2] GB/T 35770—2022 合规管理体系 要求及使用指南