《信息通信及互联网行业企业合规管理体系 指南》标准编制说明

《信息通信及互联网行业企业合规管理体系指南》标准起草组

2022 年 11 月 11 日

1、　标准范围。

《信息通信及互联网行业企业合规管理体系指南》（以下简称本标准）规定了信息通信及互联网企业建立、实施、评估、维护及改进企业合规管理体系的总体要求。本标准适用于开展合规管理相关工作的信息通信及互联网企业。

2、　工作简况。

随着经济全球化的发展和企业治理体系的不断演变，全球合规治理领域的内涵和组成也在快速的变化。为了提升各类组织的合规管理规范化水平，促进全球经济交流与合作，2014 年 12 月，国际标准“ISO19600：2014 Compliance Management Systems Guidelines” 正式发布,2020 年 11 月 ISO 完成该标准的修订工作,发布“ISO 37301：2020 合规管理体系 要求及使用指南”。我国高度重视企业现代管理制度建设和企业经营行为合规制度建设。早在 2017 年 5 月 23 日，中央全面深化改革领导小组第三十五次会议上,就讨论了中国企业面临合规挑战的新问题。2017 年国家标准化委员会依据 ISO 19600：2014 国际标准，发布编号为 GB/T35770 的《合规管理体系 指南》，为我国企业合规的进一步发展奠定了良好的理论基础和行为指南；2021 年，随着国际标准 ISO:37301 的更新，GB/T35770 的修订更新工作也相应启动，截止目前，修订后的国家标准《合规管理体系 要求及使用指南》刚刚结束公开征求意见，今年 10 月份发布。更新后的标准为企业主体提高自身合规管理能力提供了系统化的方法，为司法、监管机构采信企业合规实践提供了相应的参考依据，同时，它也为便利

全球贸易、交流、合作提供了良性的通用准则。

近年来，全球针对信息通信和互联网行业的监管日益加强，企业合规的要求和复杂程度也日益提高，行业迫切需要相关协会组织出台指导行业开展合规工作的标准、指南、指引，以便辅导企业更好的符合行业监管和服务社会的要求。标准编写组汇集了行业 30 多家主要企业的专家，深入研究互联网行业合规管理诉求，紧密跟踪国际和国内标准的进展情况，在 2022 年 6 月完成标准大纲架构，7 月组织起草组和行业主要企业，讨论标准中专项合规的主要内容和编写困难，9 月底完成征求意见稿的编写和评审工作。后续根据公开征求意见继续完善标准的编写工作。

3、 标准编制原则和确定标准主要内容的依据。

标准编制遵循的原则和主要内容依据主要有三点：一是全面吸收国际标准和国家标准对合规管理体系的相关要求，在标准整体架构上，和 ISO 37301:2020 和 GB35770 保持尽可能一致，重点对与信息通信和互联网行业相关的重点专项合规进行规定；二是体现产业合规要求的行业特色和时代特色，坚持走中国道路，在合规领域兼顾行业发展和安全，注重互联网平台治理、业务合规、数据安全与个人信息安全等要求；三是聚焦互联网和数字经济领域的重点要求，以合规打造互联网行业“新”生态，加强企业合规自律管理，培育和传播积极的合规文化，树立诚实守信的企业形象，有效防范重大经营风险，注重产业创新发展的可持续性。

4、主要试验（或验证）的分析、综述报告。

合规管理体系的国际标准的起源是澳大利亚国家标准 AS 3806《合规计划》。随着该标准被全球接纳程度越来越高，制定国际性的企业合规管理标准逐渐成为大家的共识和需求。2012 年 10 月，国际标准化组织（ISO）成立 ISO/PC271 合规管理项目委员会，正式启动合规管理体系的国际标准制定工作。2014 年 12 月，国际标准“ISO19600：2014 Compliance Management Systems Guidelines”正式发布。

2016 年 5 月，我国合规管理体系的国家标准制定正式启动，基本编制原则为等同采用 ISO 19600。2017 年 12 月 29 日正式发布我国的合规管理体系国家标准 GB/T 35770-2017《合规管理体系 指南》。随着经济全球化的发展和企业治理体系的不断演变，全球合规治理领域的内涵和组成也在快速的变化，需要对原有标准进行修订。2020 年 11 月 ISO 完成修订工作，发布 ISO 37301：2020《合规管理体系 要求及使用指南》。而我们国家也与 2020 年启动相应的国标编制工作，于 2022 年 10 月发布。

近年来，全球针对信息通信和互联网行业的监管日益加强，企业合规的要求和复杂程度也日益提高，行业迫切需要相关协会组织出台指导行业开展合规工作的标准、指南、指引，以便辅导企业更好的符

合行业监管和服务社会的要求。标准编写组高度重视行业的诉求，并紧密跟踪国际和国内标准的进展情况，适时启动本团体标准的编写工作。

本标准是指导信息通信和互联网企业组织建立、运行、维护和改进其合规管理体系的规范化框架，通过构建组织、文化和赋权，将合规治理融入企业的的日常经营、决策，并保证其独立性，以满足外部监管对企业合规治理的要求；标准贯彻 PDCA 理念，将策划—执行—检查—改进闭环流程融入整个合规管理体系；通过组织机构和业务过程中的风险识别开展有针对性的管理措施，降低风险发生概率，从而满足合规管理要求。本标准沿用了 ISO 37301：2020 的文件结构和主要通用要求，但在合规内容方面，根据行业特点重新进行了梳理和归纳，分别从数据安全与管理、个人信息保护、出口管制、网络安全等 16 个方面对合规依据、管理职责、主要风险点、管理原则和方针、以及合规管理关键措施进行了说明。

5、标准在起草过程中遇到的问题及解决办法：重大分歧意见的处理经过和依据：有无重要技术问题需要说明。

标准起草过程中，起草组主要成员就是专项合规的项目选择、编制内容的详略程度、以及各专项合规的管理方法，均展开了充分的讨论，在综合考虑要求的通用性和具体工作的实操性方面达成了一致。主要讨论经过参见意见汇总表。

暂无重要技术问题需要说明。

6、与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异（可引用标准前言的内容）：

无国外标准直接采用。ISO 37301：2020 合规管理体系 要求及使用指南仅在文件结构和主要通用要求方面，给本标准提供了借鉴。

7、修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条（可引用标准前言的内容）：废止/代替现行有关标准的建议：

非修订标准。

8、说明标准与其他标准或文件的关系（可引用标准前言的内容），特别是与有关的现行法律、法规和强制性国家标准的关系：

本标准在数据合规和个人信息保护合规部分，严格按照《数据安全法》和《个人信息保护法》的相关条款进行了企业合规任务的梳理，此外，ISO 37301：2020 在文件结构和主要通用要求方面，给本标准提供了借鉴。

9、标准作为强制性标准或推荐性标准的建议：

本标准建议作为推荐性标准使用。

9、贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）：标准发布后，对国内外业界可能产生的影响。

本标准主要规定了信息通信及互联网企业建立、实施、评估、维护及改进企业合规管理体系的总体要求。标准发布后，将组织标准宣贯和研讨会，组织信息通信和互联网企业参加；同时通过开展专项合规培训和能力建设，辅导企业按照标准进行合规能力建设；第三，通过企业合规推进计划，组织企业自愿参加标准符合性活动，推动企业内部合规管理体系建设。

11、标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程。

标准不涉及知识产权。

12、其他应予说明的事项。

无。