附件 2

团体标准《网络安全保险风险评估规范》编制说明

一、工作简况

1.任务来源

随着数字化转型的深入和网络攻击事件的频发，网络安全保险作为转移网络风险的重要金融工具，市场需求日益增长。为规范网络安全保险承保前的风险评估流程，统一评估标准与方法，提升评估工作的科学性和一致性，中国人民财产保险股份有限公司深圳市分公司，于 2025 年 9 月向深圳市网络与信息安全行业协会提出《网络安全保险风险评估规范》团体标准立项申请。深圳市网络与信息安全行业协会按程序批准该团体标准立项并发布公告。来自中国人民财产保险股份有限公司深圳市分公司等单位的专家参与了标准的制定。

2.编制目的

当前，我国网络安全保险市场尚处于发展初期，在风险评估环节存在评估维度不统一、评估方法多样化、评估结果差异大等问题，这不仅影响了保险公司对网络风险的精准定价和有效承保，也使得投保企业难以清晰了解自身的风险敞口和改进方向。本标准的编制目的在于：建立一套科学、规范、可操作的网络安全保险风险评估框架和方法论，为保险机构、网络安全服务商和投保企业提供统一的作业指引。通过规范风险评估的流程、内容和标准，旨在解决评估标准缺失、评估过程不透明的问题，促进网络安全保险市场的健康、有序发展，最终提升全社会网络风险管理的整体水平。

二、标准的属性

本标准为深圳市网络与信息安全行业协会制定发布的团体标准。

三、标准制定原则

按照 GB/T1.1-2020《标准化工作导则 第 1 部分:标准化文件的结构和起草规则》的要求和规定编写本标准内容。

本标准具有先进性、系统性、普适性、可操作性。

三、确定标准主要内容的依据

1.法律法规要求

《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，明确了网络运营者的安全保护义务。这些法定义务是衡量企业网络安全合规性的基本准绳，也是网络安全保险风险评估的核心基线。

本标准将相关法律法规的合规性要求作为风险评估的重要组成部分，确保评估工作与国家法律体系保持一致。

2. 行业最佳实践

本标准融合了网络安全与保险两大行业的最佳实践。在网络安全方面，参考了如GB/T 45576-2025 网络安全技术 网络安全保险应用指南、NIST SP 800-30 风险评估指南、ISO/IEC27005 信息安全风险管理框架等国内外公认的成熟框架；在保险方面，借鉴了传统财产保险的核保风控模型和管理经验。通过跨界融合，形成一套既符合网络安全技术逻辑又满足保险精算要求的评估体系。

3.技术发展趋势

勒索软件、供应链攻击、数据泄露等已成为当前网络安全的主要威胁，也是网络安全保险理赔的主要原因。本标准紧跟技术发展和攻击手段演变趋势，将针对高级持续性威胁（APT）、数据安全态势、应急响应与恢复能力等方面的评估作为重点内容，确保标准能够有效应对新型网络风险。

4.专家意见和学术研究

标准编制组征求了来自保险公司核保部门、网络安全评估机构、企业首席信息安全官及法律顾问的意见。通过多轮研讨和市场调研，深入了解了当前风险评估工作中的痛点和需求，如评估效率、成本控制、结果互认等，并将这些实际需求融入标准条款，确保标准的实用性和市场接受度。

五、国内外现有相关标准情况

目前，国内外尚未形成一个统一的、被广泛采纳的，专门为网络安全保险承保风险评估而设计的标准。

国际上，ISO/IEC 27000 系列标准定义了信息安全管理体系，NIST 网络安全框架

提供了风险管理的指导，但它们主要面向企业自身安全建设，未直接关联保险承保的具体需求，如风险量化、可保性分析等。

国内，GB/T 22239《信息安全技术网络安全等级保护基本要求》、GB/T 32914《信息安全技术网络安全服务能力要求》、GB/T 24364《信息安全技术信息安全风险管理实施指南》等标准是评估网络运营者安全能力的重要依据。

然而，上述现有标准均未系统性地规定从保险视角出发，如何对一个组织的网络风险进行全面的、标准化的评估，以支持保险产品的定价、承保和理赔。本标准旨在填补这一空白，将通用的网络安全要求转化为可用于保险业务的、具体的风险评估指标、流程和方法，为网络安全与保险的深度融合提供关键的标准支撑。

六、重大分歧意见的处理经过和依据

本标准在制定过程中未出现重大分歧意见。

七、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发布实施。

八、其他应予说明的情况

无。