中国网络安全产业联盟标准

《网络安全保险 安全风险评估实施指南》（征求意见稿）

编制说明

一、工作简况

1、 任务来源

现阶段网络安全服务提供方与保险机构合作开展网络安全保险业务时，对潜在投保用户的信息系统缺乏有效的网络安全风险评估过程、指标和方法，极大影响网络安全保险在国内的推广和应用，制约网络安全产业生态健康有序发展。为规范网络安全保险保前风险评估，广泛征求中国网络安全产业联盟（CCIA）成员意见后，经 CCIA 秘书处批准立项开展《网络安全保险 安全风险评估实施指南》联盟标准的研制工作。

2、 标准编制的主要成员单位

本标准由杭州安恒信息技术股份有限公司负责起草，参与起草单位有北京天融信网络安全技术有限公司、绿盟科技集团股份有限公司、亚信科技（成都）有限公司、北京知道创宇信息技术股份有限公司、上海观安信息技术股份有限公司、北京梆梆安全科技有限公司、北京瑞和云图科技有限公司、北京六方云信息技术有限公司等。

3、 主要工作过程

① 杭州安恒信息技术股份有限公司牵头在 CCIA 立项《《网络安全保险 安全风险评估实施指南》标准，于 2021 年 4 月面向会员单位公开征集参编单位。共征集到参编意向的企业 34 家。

② 2021 年 7 月 29 日，标准工作组在北京召开了标准起草会，来自 15 家参编单位的 18 位专家代表参加了本次会议，会议对《网络安全保险 安全风险评估实施指南》标准草案大纲、风险评估框架、业务流程及征集到的建议等内容进行了讨论，对标准大纲，投保阶段的风险评估框架和业务流程初步达成一致意见，完成标准初稿 1.0 版本。

③ 2021 年 9 月 2 日《网络安全保险 安全风险评估实施指南》标准编写组在北京召开了标准编写工作会。来自 11 家参编单位的 13 位专家代表参加了本次会议，本次会议根据标准编制流程，会议对前一阶段各编制单位反馈意见进行了讨论和处理。研究和讨论了风险值计算方法，形成《网络安全保险 安全风险评估实施指南》标准初稿 2.0 版本。

④ 2021 年 10 月-11 月，编制组在线上召开两次讨论会，针对风险计算方法、脆弱性识别和已有控制措施识别与权重赋值等问题进行了研究和验证，形成初稿 3.0 版本。

⑤ 2021 年 11 月 26 日，中国网络安全产业联盟在北京组织召开专家审查会，对联盟标准《网络安全保险 安全风险评估实施指南》（初稿）进行了技术审查，标准牵头研制单位杭州安恒信息技术股份有限公司汇报了标准研制过程和主要技术内容，专家组对标准主要技术内容进行了质询，并建议加强标准与具体保险业务、重点险种的关联性，提高标准针对性。

⑥ 2021 年 12 月，标准牵头研制单位杭州安恒信息技术股份有限公司组织编制核心参编单位，结合专家审查会提出的修改建议，将网络安全保险风险评估进行了通用场景下的风险计算和典型场景下的风险计算相结合，重点对现有数据安全场景、网络勒索场景和业务连续性中断场景的风险计算进行了规范，加强了对具体保险业务，重点险种的关联性，增强了标准可用性。形成本标准征求意见稿。

二、标准编制原则和确定主要内容的论据及解决的主要问题

1、标准制定的基本原则

在标准制定过程中，主要遵循了以下原则：

① 贯彻国家有关政策法规要求；

② 与已颁布实施的相关标准兼容协调；

③ 广泛征求专家、联盟成员、保险机构和管理部门的意见；

④ 理论与技术相结合，平衡标准的先进性和实用性，注重标准可操作性；

2、确定主要内容的依据

标准的制定主要依据：

1) 标准格式按照 GB/T1.1—2020 标准要求编写。

2) 本文件制定引用并参考以下国家标准：

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 31509 信息安全技术 信息安全风险评估实施指南

GB/T 36687-2018 保险术语

GB/T 31722-2015 信息技术 安全技术 信息安全风险管理

GB/T 36466-2018 信息安全技术 工业控制系统风险评估实施指南

GB/T 36637-2018 信息安全技术 ICT供应链安全风险管理指南

GB/T 37988-2019信息安全技术　数据安全能力成熟度模型

信息安全技术 关键信息基础设施安全防护能力评价方法（征求意见稿）

3、 解决的主要问题

网络安全风险具有不可绝对消除性，分散、转移风险作为网络风险管理的一环，重要性日益增强。网络安全保险作为风险转移的重要手段，得到越来越多的关注。现阶段开展网络安全保险业务时，对潜在投保用户的信息系统缺乏有效的网络安全风险评估过程、指标和方法，极大影响网络安全保险在国内的推广和应用。本标准通过建立一套风险评估指标、流程、内容，规范对拟投保标的的风险评估，评估风险等级、计算风险分值，从而能够定量化的显示标的物网络安全风险状况，为后续开展网络安全保险业务提供参考依据。

本文件规范了网络安全保险投保阶段的网络安全风险评估实施过程，规范了网络安全保险通用场景和数据安全、网络勒索和业务连续性中断三类典型场景的风险计算方法。

标准初稿共为8章，第1-3章分别为范围、规范性引用文件和术语定义。第4章对网络安全保险安全风险评估进行了概述，包括网安保险风险评估的基本原则、实施方法、险别分类和投保流程。第5规范了网安保险风险评估实施流程，将风险评估实施划分为评估准备、要素识别、风险分析与风险处理四个阶段，在网安保险实践中，通常将交付保险公司核保作为风险处理阶段；针对要素识别、风险分析两个核心阶段，标准第6章详细规范要素识别，包括业务识别、资产识别、威胁识别、脆弱性识别以及权重赋值方法；第7章规范典型场景下网络安全保险风险值量化计算的方法。第8章针对数据安全、网络勒索和业务连续性中断三类典型场景下提出网络安全保险风险量化计算方法。在附录A给出通用场景下脆弱性识别和权值赋值参考，在附录B给出通用场景下已有安全控制措施识别与赋值参考，在附录C给出三类典型场景已有安全控制措施识别参考，附录D给出实践案例。

本标准适用于指导网络安全服务提供商在网络安全保险投保阶段开展网络安全风险评估活动。可为保险公司、再保险公司开展网络安全保险业务前的风险评估与风险定价等提供指导，为网络安全保险投保人或被保险人开展网络安全风险自评估提供参考

三、主要试验情况分析

2021年11月已针对标准初稿内容做内部测试。

四、专利情况说明

本文件不涉及专利。

五、产业化情况、推广应用论证和预期达到的经济效果

网络安全保险作为企业信息安全控制体系的风险应对方式之一，可以有效降低网络安全事件的影响，提高企业应对风险的“韧性”，通过保险结合技术的方式，不仅在保前、保中环节做好企业安全防护，在发生网络安全事件并造成经济损失时，可通过保险损失补偿功能，赔付企业损失，尽快恢复正常生产经营秩序，是企业建立网络安全风险整体保障机制的重要组成部分。

通过建立一套网络安全保险风险评估指标，指导、规范网络安全保险投保前风险评估工作，分析与量化企业安全风险，形成贴合投保企业实际风险场景的网络安全保险保单。

六、采用国际标准和国外先进标准情况

无。

七、与现行相关法律、法规、规章及相关标准的协调性

本文件与现行法律、法规、强制性国家标准及相关标准协调一致。本文件整体框架、识别指标借鉴 GBT 20984-2007《信息安全技术 信息安全风险评估规范》和 GB/T 31509《信息安全技术 信息安全风险评估实施指南要求》，并创新性的将保险险别、投保信息系统等因子纳入风险评估参考指标中，将信息安全风险评估一般方法与保险特殊属性相结合，体现网络安全保险标准的侧重点。同时将定量化分析作为主要的评估手段，在评估结果中输出投保信息系统风险等级、风险分值作为评判指标。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议

建议作为联盟标准发布。

十、贯彻标准的要求和措施建议

本文件主要通过标准化的形式来将网络安全保险投保前安全风险评估进行规范，有助于网络安全产业生链发展，完善生态。

十一、替代或废止现行相关标准的建议

无。

十二、其他应予以说明的事项

无。

《网络安全保险 安全风险评估实施指南》编制工作组

2021-11-24