一、工作简况

1.1 任务来源

根据国家标准化管理委员会2023年下达的国家标准制修订计划,《信息安全技术 网络安全保险应用指南》由北京源堡科技有限公司负责承办，计划号：20230794-T-469。本标准由全国信息安全标准化技术委员会归口管理。

1.2 制定背景

随着社会信息化程度的不断加深，数字经济的快速发展，网络安全风险也在持续演变，为世界经济带来了广泛而深远的影响。作为应对网络安全风险的手段之一，网络安全保险受到各国政府和组织的高度重视。网络安全保险是组织实现风险转移的一种有效手段，其在转移潜在风险、优化资源配置、保障组织财务稳定性和业务连续性等方面发挥着重要作用，也逐渐成为组织网络安全风险管理的组成部分。国外网络安全保险发展相对成熟，组织在应对网络安全风险时，通常会将保险作为一种风险处置方式纳入组织的整体风险应对策略中。因此，国际标准化组织ISO/IEC、ITU-T相继制定了ISO/IEC 27102:2019《信息安全管理 网络保险指南》、ITU-T X.1061 (08/2021)《网络保险获取指南》等国际标准，对组织如何投保网络安全保险进行指导。

2021年7月，工业和信息化部发布《网络安全产业高质量发展三年行动计划》（征求意见稿），提出“探索开展网络安全保险，加快网络安全保险政策引导和标准制定，通过网络安全保险服务监控风险敞口”。2023年7月，工业和信息化部和国家金融监管总局发布《关于促进网络安全保险规范健康发展的意见》（以下简称《意见》），提出“建立覆盖网络安全保险服务全生命周期的标准体系，明确承保、核保、理赔等主要环节基本流程和通用要求。研究制定承保前重点行业领域网络安全风险量化评估相关标准，规范安全风险评估要求”。

在上述背景下，为落实国家《网络安全法》，加强对网络安全风险监管，积极推动网络安全保险及服务模式的创新和发展，响应《意见》要求，本文件借鉴了国际网络安全保险相关标准成果，结合我国网络安全保险产业现状和网络安全风险管理实践，提出适合我国国情的网络安全保险应用指南，帮助并指导组织通过网络安全保险应对和管理风险。基本思路如下：

1）从网络安全保险应用的角度，帮助各参与方认识和理解网络安全保险的基本概念和作用，阐述网络安全保险不同阶段中的安全技术的应用，切实为参与方应用网络安全保险提供可操作性的指导。

2）阐述网络安全保险的基本概念，形成保险的作用和目的的统一理解，从网络安全角度的描述可保的网络安全事件和相关损失，以及和保险保障范围的关系，为理解保险能够解决什么问题提供参考。

3）明确网络安全保险应用的主要阶段及技术应用的特点，并针对每个阶段安全技术的应用特点，提出基本内容和方法，帮助投保组织、保险人和技术服务提供商理解保险应用中安全技术差异性和侧重点，为实施提供指导。

1.3 起草过程

北京源堡科技有限公司负责组织起草，国家工业信息安全发展研究中心、中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、国家信息中心、公安部第一研究所、公安部第三研究所、中国科学院信息工程研究所、中国网络空间研究院、中国人民财产保险股份有限公司、中国太平洋财产保险股份有限公司、中国平安财产保险股份有限公司、中国人寿财产保险股份有限公司、国任财产保险股份有限公司、诚泰财产保险股份有限公司、中国财产再保险有限责任公司、前海再保险股份有限公司、建信财产保险有限公司、奇安信科技集团股份有限公司、北京神州绿盟科技有限公司、启明星辰信息技术集团股份有限公司、北京天融信网络安全技术有限公司、杭州安恒信息技术股份有限公司、腾讯云计算（北京）有限责任公司等单位共同参与了本标准的起草工作。具体起草过程如下：

（1）标准草案阶段

1） 2020 年 3 月-2021 年 4 月，标准预研并初步组件标准编制组，形成标准草案初稿，并参与 2021 年 5 月的标准会议周立新答辩。

2） 2021 年 6 月至 8 月，根据标准会议周相关意见，完善标准草案，同时于 7 月 9 日召开专家研讨会议及标准编制组内部会议，根据标准意见，修改完善标准草案。

3） 2021 年 12 月至 1 月，召开 4 次标准编制会议，重新梳理标准框架并完善分工，并组织一次专家研讨，继续完善标准草案。

4） 2022 年 1 月 20 日，信安标委秘书处组织重点标准项目阶段检查，专家提出标准审查意见。根据专家意见，对标准草案进行进一步完善。

5） 2022 年 1 月 21 日-3 月 8 日，根据专家审查意见重新修订标准草案内容框架和文本内容，形成申报立项的标准草案版本（v0.9）。

6） 2022 年 3 月，信安标委发布《信息安全技术 网络安全保险应用指南》编制需求工作的通知。在网络安全管理工作组 WG7 立项申请和答辩。

7） 2022 年 3 月 9 日-3 月 18 日，组织标准立项申报，扩展标准编制工作组，于 3 月 18 日召开标准编制全体会议讨论标准草案，形成标准草案（v0.95）。

8） 2022 年 4 月 19 日，通过信安标委组织的标准立项答辩。

9） 2022 年 6 月，召开标准编制全体会议，讨论标准草案（v0.95），收集意见，继续完善标准草案（v1.0）。

10）2022 年 12 月 5 日，在信安标委 2022 年会议周 WG7 工作组会议上汇报标准编制的进展情况，听取与会专家的意见，经工作组讨论决议，同意转征求意见稿。

（2）标准征求意见稿阶段

1） 2022 年 12 月 10 至 12 月 20 日，处理会议周意见，形成标准征求意见稿（v1.1）。

2） 2022 年 12 月 23 日，召开编制组线上会议，继续完善标准，形成标准征求意见稿（v1.2）。

3） 2023 年 1 月 24 日-2 月 10 日，处理责任编辑和责任专家意见，继续完善标准草案文本（v1.5），通过了责任专家和责任编辑的标准文本质量把关，提交工作组，准备专家评审会。

4） 2023 年 3 月 14 日，在信安标委专家评审会上汇报标准编制的进展情况，充分听取专家评审意见。

5） 2023 年 3 月 23 日，在北京源堡科技有限公司召开标准专家讨论会，邀请安标委秘书处专家进行现场指导，讨论专家评审会上所提修改意见的修改情况。

6） 2023 年 4 月 7 日和 5 月 6 日，召开两次标准专家研讨会，针对评审

会意见进行讨论，继续完善标准，形成标准征求意见稿（v1.6 和 v1.7）。

7） 2023 年 6 月 1 日，在信安标委 2023 年工作组标准会议周上，汇报标准进展及编制情况，收集与会专家修改建议。

8） 2023 年 6 月 2 日-8 月 3 日，针对评审会专家意见和会议周专家意见，对标准进行修改，成标准征求意见稿（v1.8 和 v1.9）。8 月 3 日提交标准工作组。

9） 2023 年 8 月 4 日，参加信安标委组织的专家评审会，再次听取专家对标准的修改意见，与会专家同意通过对该项标准的审查，建议根据会议意见修改后，发起公开征求意见。

10） 2023 年 8 月 5-24 日，根据 8 月 4 日专家评审会意见进一步修改标准文件，提交信安标委，形成公开征求意见稿（v2.0）。

二、标准编制原则、主要内容及其确定依据

2.1 标准编制原则

本标准的研制工作遵循以下原则：

1)规范性：严格按照国家标准编制流程和国家标准规范 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》的规定进行标准的编制工作，力求达到编制的标准思路清晰、逻辑合理、文本规范、内容完整；

2)可操作性和实用性：本标准适用于国内网络安全保险相关工作的组织和开展，且符合我国基本国情，力求标准在具体执行中具有较好的可操作性和实践指导价值；

3)协调一致性：广泛征求业界专家的意见，同时充分考虑与现有相关标准的关联关系，力求达到编制标准的不同使用方的协调一致和国内外相关技术标准协调一致；

4)科学性与先进性：借鉴国际网络安全保险领域前沿研究成果和规范性文献的科学方法及思路，进行标准文本的设计和编写。

2.2 主要内容及其确定依据

主要内容依据：

GB/T 20984—2022　信息安全技术　信息安全风险评估方法

GB/T 20986—2023　信息安全技术　网络安全事件分类分级指南

GB/T 22081—2016　信息技术 安全技术 信息安全控制实践指南

国内网络安全保险市场正处于起步阶段，参考国外市场的成熟经验，国内已逐步开展网络安全保险业务，但由于缺乏对相关概念、流程和方法相关的标准，导致在实际业务开展过程中存在诸多问题。一方面对于市场需求方的投保企业而言，如果没有清晰的理解网络安全保险对于风险管理的作用是什么，通过网络安全保险能够转移哪些网络安全风险，以及当发生哪些网络安全事件所导致的损失能够通过保险赔偿，对于网络安全保险中的保障范围等概念包括哪些内容等等问题，都会对投保企业真正应用网络安全保障带来障碍。另一方面，对于市场供给方的保险公司而言，网络安全保险属于财产险范畴，但网络安全风险却与传统财产险中的风险有很大区别，保险公司从损失的角度看待风险与企业看到的网络安全风险也存在理解上的差异，如不能直接将损失与投保企业的安全问题和可能发生的安全事件直接对应，因此会导致在网络安全保险的实际应用过程中，风险评估的技术方法和目的，是否需要采用风险控制，以及在出险后如何应对等均在应用的难点，从而使得保险公司在承保网络安全风险时持谨慎态度，也不利于网络安全保险供给的释放，不利于市场的健康发展。

针对当前国内网络安全保险市场应用方面实际存在的问题，本标准将从网络安全保险的实际应用过程出发，切实解决投保企业对于网络安全保险缺乏统一理解，对网络安全风险和保险保障范围认知差异较大，以及网络安全保险应用中的基本方法等问题，帮助投保企业、保险公司以及第三方技术服务方等参与者更好的理解和应用网络安全保险，促进应用的规范化，也提高市场供需能力。本标准主要解决问题包括：

（1）解决当前网络安全保险供需双方对于网络安全保险目的和概念的理解差异性问题，如可承保的网络安全事件、损失类型和网络安全保障范围等，指导投保企业（需求方）和保险机构（供给方）在网络安全保险应用充分理解需求目标，促进网络安全保险市场的发展。

（2）解决网络安全保险应用过程中的流程规范化问题，如网络安全保险应用的通常环节，每个环节参与方的角色和作用等，指导投保企业、保险机构以及服务方在应用中明确各自的定位、作用和任务。

（3）解决网络安全保险中所应用的基本安全技术方法以及差异性问题，如投保前开展风险评估内容和方法，保险中风险监测目的和内容，以及出险后事件评估的基本内容和作用等。指导各参与方能够根据标准基本实现网络安全保险应用的过程。

根据《意见》中提到的：“建立覆盖网络安全保险服务全生命周期的标准体系，明确承保、核保、理赔等主要环节基本流程和通用要求”。本标准作为首个该领域的国家标准，定位于网络安全保险应用的通用指南性标准，重点阐述网络安全保险基本应用流程和可操作的指导性方法，侧重保险应用的过程和方法。目的是在国内网络安全保险应用的初级阶段，能够明确网络安全保险的基本应用流程和通用方法，指标并规范各参与方开展网络安全保险的应用实施。同时本标准也将对后续研究制定保险中网络安全风险量化评估相关标准，规范安全风险评估要求、风险监测管理和预警、承保后理赔服务实施等技术要求提供总体性指导，从而逐步覆盖建立网络安全保险全生命周期的标准体系。

围绕上述问题，本标准主要内容包括：

（1）阐述网络安全保险概念及对风险管理的作用，明确可以通过保险转移的网络安全事件和主要损失类型，建立网络安全风险与保险保障范围的关系。解决当前网络安全保险供需双方对于网络安全保险目的和概念的理解差异性问题。

（2）阐述网络安全保险应用的主要环节以及主要参与方，各参与方的主要作用和职责。解决网络安全保险应用过程中的流程规范化问题。

（3）提出在网络安全保险应用主要环节中的基本方法和内容，对投保前风险评估、保险期间风险控制以及出险后事件评估等给出基本的方法和内容，为不同环节中的保险应用提供可操作性的指导建议，解决网络安全保险中所应用的基本安全技术方法以及差异性问题。

2.3 修订前后技术内容的对比

非修订标准。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

3.1 试验验证的分析、综述报告

本标准在编制时借鉴了国外网络安全保险投保经验，结合我国网络安全保险

发展现状和网络安全风险管理经验，提出适合我国国情的网络安全保险应用指南，帮助并指导组织通过网络安全保险应对和管理风险。编制组在编制过程中，充分听取了网络安全保险服务机构（保险公司以及再保险公司）、科研院所、测试机构的意见，考虑了网络安全保险的发展和应用情况，并推进开展标准条款的试点验证工作，主要包括北京源堡科技、国家工业信息安全发展研究中心、中国科学院信息工程研究所、中国人保、中国太保、安恒、启明星辰等企业或机构，本次试点工作主要对网络安全风险评估的基本方法和应用流程、保险保障范围内的网络安全事件类型、保险期间的风险控制措施、理赔实施流程等内容进行验证，以检验标准的适用性、合理性、先进性和可操作性等，并提出标准进一步修改完善的建议，编制形成涵盖标准验证结论的报告，促进网络安全保险服务工作的规范化和标准化，为进一步开展网络安全保险应用工作提供参考。

3.2 技术经济论证

在技术方面网络安全保险主要涉及投保前风险评估，保险期间风险监测、预警和处置以及理赔中的事件鉴定溯源等技术，基于网络安全保险的业务特点和需求，需要在评估技术方法、风险指标定义、量化分析模型、风险预测技术等方面进行创新和完善，才能支撑网络安全保险业务的健康发展。在产业化方面国外网络安全保险发展较成熟，全球网络安全保险市场在 2022 年整体保费规模达到 92 亿美元，并预计在 2025 年达到 220 亿美元。国内网络安全保险市场处于起步阶段，但呈高速增长态势，年复合增长率超过 30%。除财产险外，奇安信、360、绿盟、美创、威努特等主要网络安全企业在网络安全保险产业进行布局，依托网络安全保险提升安全产品、服务、方案的整体竞争优势。

3.3 预期的经济效益、社会效益和生态效益

本标准的实施将有利于网络安全产业的高质量发展，促进产业链各方明确专业分工和责任，依托有效的网络安全风险评估和风险监控等技术手段，推动网络安全保险在国内的快速发展，提升网络安全产业规模；有利于网络安全技术服务公司、保险公司、再保公司和投保企业各参与方对网络安全保险服务形成共同理解，服务流程有据可依，更加规范，促进网络安全保险服务市场的健康有序发展，为网络安全风险管理相关技术和服务在金融领域中的应用提供了新的方向。

经济效益：促进网络安全保险市场快速发展，增加网络安全企业收入。该标准的制定，使得投保企业、保险公司、网络安全公司等各参与方对网络安全中可保风险以及如何支持企业的风险管理工作形成共同理解，使得网络安全保险业务有章可循，更加规范；保险公司能够根据安全技术应用的结果进行差异化定价和产品创新，从而促进保险市场的健康发展，进一步增加保费规模，带动网络安全企业收入的增长。

社会效益：提升网络安全技术创新能力，标准将为网络安全技术和服务在网络安全保险业务领域中的应用提供了方向和指导。通过对投保前风险评估、保险中风险监测以及安全事故鉴定等技术的应用，使得安全技术能够支持并满足保险核保评估需求，并为保险中风险管控提供技术支撑，进一步提升网络安全技术创新能力，从而为降低全社会网络安全风险，提升整体风险防范能力提供创新技术能力支撑。

生态效益：扩大产业规模，促进产业生态发展。标准将对应用于网络安全保险中的安全技术和服务提供指导，使得保险机构能够科学的评估投保企业网络安全风险状况，并通过有效的风险控制手段，促进网络安全保险市场的快速发展；同时，保险业务的发展又将直接带动安全技术在不同领域的应用，以业务促进安全产业生态发展，做大安全产业规模。

四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况

目前国际标准化组织 ISO 于 2019 年发布了 ISO/IEC 27102：信息安全管理-网络保险指南，ITU-T 于 2021 年发布了 X.1061：网络信息安全-安全管理-网络保险采购指南。ISO27102 从风险管理角度帮助企业将网络安全保险更好地与其自身的风险管理相结合，并作为风险管理活动的一部分；X.1061 则投保企业角度为如何应用网络安全保险提供指导性意见。这些标准均描述了网络安全保险的基本概念和如何使用网络安全保险帮助组织管理风险。两项标准从投保企业的角度对网络安全保险涉及的可保风险、基本流程和注意事项等进行了描述，以帮助企业计划和购买网络保险。

现有的国际标准不适合中国实际情况，需要制定适合中国国情的网络安全保险相关标准。这种差异性，体现在法律法规的依据、解决的问题、适用的对象、

市场现状等。具体体现在：

1）标准依据的法律法规不同。由于国内外法律和标准的不同，国内外网络安全保险的承保范围和保险条款均存在较大差异。本标准在对网络安全保险概述及保险保障范围的描述中，主要以国内保险法及国内保险条款的内容为基础进行描述，与国际标准对网络安全保险承保范围的描述存在较大差异。

2）标准解决的问题存在差异。国际标准侧重采购保险过程中应注意的事项，本国标侧重为网络安全保险不同阶段（投保前、承保中、出险后等）网络安全技术的应用提供具体的指导。

3）标准的适用对象不同。国际标准主要以采购保险的投保人为适用对象，本标准除给投保人提供指导外，还包括提供安全技术支持的服务方，以及开展风险控制的保险公司。

4）国内外网络安全保险市场现状不同。国外标准涉及保险相关的定义或描述，与国内保险公司存在较大差异性。本标准综合了国内保险行业参编单位的意见，采纳了更适合国内市场形态的措辞。

五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

除上面所述 ISO/IEC 27102 以及 ITU-T X.1061，尚未发现网络网络保险相关国际标准。

六、与有关法律、行政法规及相关标准的关系

本标准与《网络安全法》的协调与配套：从国际成熟经验来看，企业购买网络安全保险，对整个安全空间产业生态起到正面积极作用。通过网络安全保险，投保方有责任对风险进行管控，并且保险方通过服务提升投保企业的网络安全建设水平，有助于提高网络安全意识和促进“网络安全的良好环境”的构建，与《网络安全法》总则保持一致。同时，标准提出的保前风险评估和保中风险监测等安全技术的应用也进一步支撑《网络安全法》中提出的建立健全网络安全风险评估和应急工作机制、加强网络安全风险的监测等要求。

与等级保护、风险评估、风险管理等国家标准之间的关系：

（1）与网络安全等级保护系列国家标准的衔接：网络安全等级保护评估结果和报告在投保前的风险评估阶段可作为评估内容和参考依据。

（2）与《信息安全风险评估方法》、《信息安全风险管理》等国家标准的关系：网络安全保险是信息按风险管理标准框架中风险转移的一种手段，同时也根据网络安全保险的业务特点对其风险评估的目的和风险管理作用进行了扩展和延伸，其具体实施技术方法也可参照信息安全风险评估方法标准

七、重大分歧意见的处理经过和依据

本标准编制过程中未出现重大分歧。

八、涉及专利的有关说明

本标准不涉及专利。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

建议本标准作为推荐性国家标准发布实施。

在正式执行本标准前，需要对标准中的条款进行宣贯，以在利益相关方之间达成对标准条款理解上的一致性。

建议在标准实施初期，引入再保险公司，以“投保组织+保险公司+再保险+服务方”组成试点示范。再保险公司作为风险分担方，能够提高保险公司的风险防御能力，从而快速开展行业试点，推动标准落地。

在实施过程中，建议组织通过采购网络安全保险服务，将保险中的网络安全风险管控服务纳入到组织的风险管理的工作中，充分发挥保险的风险分担及防灾减损的作用，体现“保险+服务”的应用模式，进一步促进组织对风险的管控，优化组织风险管理能力。

同时，从标准发布到标准实施，建议过渡期设置为 6 个月。

十、其他应当说明的事项

10.1 网络安全保险推出背景及相关政策

根据国务院关于数字经济发展情况的报告（2022 年 10 月 28 日在第十三届全国人民代表大会常务委员会第三十七次会议上），“党的十八大以来，我国深入实施网络强国战略、国家大数据战略，先后印发数字经济发展战略、“十四五”数字经济发展规划，有关部门认真落实各项部署，加快推进数字产业化和产业数字化，推动数字经济蓬勃发展。十年来，我国数字经济取得了举世瞩目的发展成就，总体规模连续多年位居世界第二，对经济社会发展的引领支撑作用日益凸

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/138140042141006104