ICS 35.240.01
CCS A 11

团　　体　　标　　准

T/SNISA 04002—2025

网络安全保险风险评估规范

Guidelines For Cybersecurity Insurance Risk Assessment

2025-XX-XX 发布　　2025-XX-XX 实施

深圳市网络与信息安全行业协会　发布

目　次

前言

本文件按照 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》的规定起草。

本文件由深圳市网络与信息安全行业协会归口。

本文件主要起草单位：中国人民财产保险股份有限公司深圳市分公司。

本文件主要起草人：（待定）

引言

在我国建设网络强国的进程中，网络安全保险作为产业生态链中不可或缺的一环，意义重要而深远。网络安全保险作为网络安全领域风险管理的重要手段，特别是“保险+服务”模式的应用，已得到越来越广泛的认可。目前，我国已形成《网络安全法》、《数据安全法》、《个人信息保护法》三法为核心的网络法律体系，为数字时代的网络安全、数据安全、个人信息权益保护提供了基础制度保障，也为网络安全保险在中国的发展提供了强有力的法律基础。为更好地发挥网络安全保险的风险分散功能和服务效能，促进网络安全保险和网络安全服务之间的有效对接，现根据国家相关法律、法规和相关服务应用标准制定本文件。

本文件的制定将为深圳乃至全国网络安全保险的风险评估提供指南，通过从风险管理角度，运用科学的方法和手段，系统地分析 IT 资产、环境、管理、人员等方面所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，有利于社会和保险消费者对网络安全保险服务质量进行监督、评价，推动网络安全保险服务质量的不断改善与提升，有效推动网络安全保险健康发展。

网络安全保险风险评估规范

1 范围

本文件建立了标准化网络安全保险风险评估框架，规范了网络安全保险风险评估的总体原则、实施流程及技术要求，促进了保险机构网络安全风险评估的专业化和标准化。

本文件可作为保险机构开展网络安全保险风险评估及网络安全技术机构提供网络安全风险评估的参考指南。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

[1] GB/T20984 信息安全技术信息安全风险评估方法
[2] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 36687-2018 保险术语
[4] GB/T20984-2022 信息安全技术 信息安全风险评估方法
[5] GB/T 24364-2023 信息安全技术 信息安全风险管理实施指南
[6] GB/T 32914-2023 信息安全技术网络安全服务能力要求
[7] GB/T 42926-2023 金融信息系统网络安全风险评估规范
[8] GB/T 42446-2023 信息安全技术 网络安全保险服务规范
[9] GB/T 45576-2025 网络安全技术 网络安全保险应用指南
[10] NIST SP 800-30 风险评估指南
[11] ISO/IEC27005 信息安全风险管理框架

3 术语和定义

下列术语和定义适用于本文件：

3.1

网络安全风险 cyber security risk

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.2

网络安全事件 cybersecurity incident

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据和业务应用造成危害,对国家、社会、经济造成负面影响的事件。

3.3

网络安全服务 cybersecurity service

根据服务协议，基于服务人员、技术、工具、管理和资金等资源，提供保障网络运行安全、网络信息安全检测等服务的相关过程。

3.4

网络安全保险 cybersecurity insurance

网络安全保险是以投保人信息资产安全性（信息的完整性、机密性、有效性等）为保险标的的保险服务产品。对由于网络安全事件给组织造成的负面影响进行赔偿，赔偿内容既包括组织本身财产损失也包含第三方赔偿责任。

3.5

网络安全服务机构 cybersecurity service provider

具有专业服务相关资质，且为网络安全保险业务提供网络安全服务(3.3)的专业机构，包括提供风险评估、风险监测、安全检测、事件鉴定、损失评估等专业服务。

3.6

保险人 insurer

与投保人订立保险合同共同分担网络安全风险，并承担赔偿或者给付保险金责任的保险公司。

3.7

被保险人 insured

向保险人分担或考虑分担网络安全风险的法人主体，其财产受保险合同保障，享有保险金请求权。

4 网络安全风险评估概述

网络安全保险风险评估是保险人及网络安全服务机构，为支撑网络安全保险的核保定价、过程风险管理及理赔定损等核心环节，运用系统化方法识别、分析、量化投保人/被保险人面临的网络安全风险的过程。其核心目标是准确评估风险敞口，为保险决策提供依据，并促进被保险人提升网络安全水平。

4.1 风险分类

网络安全保险主要承保的风险涵盖第一方损失风险及第三方责任风险两大类别。

4.1.1 第一方直接损失风险

指网络安全事故直接导致的被保险人自身财产损失或费用支出，具体包括：

a）营业中断损失：因恶意程序、网络攻击等网络安全事件导致关键业务系统中断或关键数据损毁，造成的经营性收入损失及业务恢复期间的额外成本支出；

b）网络勒索损失：因计算机系统遭受安全威胁造成的勒索损失，包括勒索款项、谈判等危机管理费用及相关调查费用。

c）数据资产损失：因网络安全事故造成企业数据丢失从而产生的数据评估、恢复等相关费用；

d）应急响应费用： 事件发生后立即产生的必要费用，包括应急响应服务费、事件调查费、公关费用、依法向监管机构及受影响的个人/实体进行通知的费用等。

4.1.2 第三方责任风险

指因被保险人的网络安全事故导致第三方业务业务中断、信息泄露等依法应由被保险人承担经济赔偿责任的风险。主要包括：

a）网络安全责任：

因被保险人网络安全事件导致第三方业务中断等非信息泄露损失，依法应承担的经济赔偿责任；

b）信息泄露责任：

因被保险人疏忽或过失导致第三方敏感信息（如个人隐私数据、商业秘密）等发生泄露损，依法应承担的经济赔偿责任。

4.2 风险来源

从风险来源来看，网络安全风险可以分为内部风险、外部风险及环境风险。

4.2.1 内部风险

内部风险是指来自内部人为管理因素造成的安全风险，主要包含以下类型：

a）管理制度缺陷：安全管理制度体系不健全或未有效执行，缺乏专职安全岗位或职责不清；

b）技术管控失效：包括但不限于信息系统维护失当、配置错误、补丁更新滞后等系统性运维缺陷；

c）权限管理失控：身份认证机制缺陷、授权策略失当或权限分配混乱导致的非授权访问风险；

d）数据保护漏洞：因数据分类分级缺失、加密保护不足或访问控制失效导致的敏感信息泄露；

e）人员行为风险：员工安全意识不足、弱密码使用、安全政策执行不力等人为因素风

险；

f）供应链风险：对外包服务商及供应链缺乏有效安全评估和持续监督机制；

4.2.2 外部风险

外部风险主要是指来自外部实体或环境对组织或系统造成的安全风险，主要包含以下类型：

a）非法入侵攻击：未经授权的外部实体通过网络渗透手段获取系统控制权；

b）勒索软件攻击：通过加密劫持关键业务数据实施财物勒索的定向攻击；

c）恶意代码传播：病毒、木马、蠕虫等恶意程序导致的系统破坏或数据窃取；

d）高级持续性威胁：有组织、有策略的持续性网络攻击活动；

e）拒绝服务攻击：通过流量泛洪攻击致使目标系统服务不可用的资源耗尽型攻击；

f）无线网络渗透：利用无线通信协议漏洞实施的中间人攻击、破解无线网络密码进行非法访问；

j）社会工程攻击：通过心理操纵或欺骗手段诱导目标人员泄露敏感信息或执行危险操作。

4.2.3 环境风险

环境风险主要是因外部环境的不规则变化影响或导致风险事故的发生，主要包含以下类型：

a）自然灾害风险：地震、洪水、火灾等不可抗力导致的基础设施物理损毁；

b）基础设施故障：电力中断、通信网络瘫痪等公共服务异常引发的业务连续性风险；

c）地缘政治风险：国际局势动荡、网络空间军事冲突等引发的系统性安全危机；

d）技术变革风险：AI 攻防等新技术演进带来的新型威胁挑战；

e）法律政策风险：数据跨境传输、网络安全审查等法律法规变化导致的运营风险。

4.3 风险评估参与主体

网络安全保险作为有效转移网络安全风险的工具，能够帮助企业建立全面的网络安全风险应对方案。网络安全保险风险评估涉及多方协作，包括投保人、被保险人、保险人及网络安全服务机构四大主体。

a）投保人：指与保险人订立保险合同，并按照合同约定负有支付保险费义务的人。投保人为自己投保时，投保人即被保险人；投保人为其他法人主体投保时，投保人代被保险人缴纳保费，投保人和被保险人是不同法人主体。

b）被保险人：向保险人分担或考虑分担网络安全风险的法人主体，其财产受保险合同保障，享有保险金请求权。被保险人是网络安全风险的主要承担者及网络安全保险直接受益人。

c）保险人：指与投保人订立保险合同，并按照合同约定承担赔偿或者给付保险金责任的保险公司。

d）网络安全服务机构：

网络安全服务机构是指为网络安全保险业务提供网络安全服务的专业机构，包括提供风险评估、风险监测、安全检测、事件鉴定、损失评估等专业服务。保险人应对网络安全服务机构通过科学的评估体系进行筛选，网络安全服务机构评估体系可见附录 B。

5 网络安全保险风险评估框架

5.1 风险评估原则

网络安全风险评估应遵循以下原则

a）全面性原则：评估应涵盖技术、管理、运营等各个方面，确保全面识别潜在风险；

b）动态性原则：评估应考虑到风险随时间和环境变化的特性，反映动态风险态势；

c）可操作性原则：评估方法、指标和结果应清晰、具体，为实际业务决策提供有力支持；

d）可追溯性原则：应详实记录评估过程和结果，便于审查和改进；

e）保险导向性原则：评估应紧密围绕保险责任范围、核保定价、理赔定损等保险核心环节展开。

5.2 风险评估通用流程

5.2.1 启动阶段

a）明确评估目的和范围，确保评估工作的方向性与目标一致；

b）确定评估团队和方案，保证评估工作的专业性和高效性；

c）制定评估计划和时间表，确保各项工作按时完成；

d）获得投保机构的授权，为评估工作提供合法依据。

5.2.2 信息收集阶段

a）识别和分类信息资产（如：客户数据、财务数据、关键系统）；

b）识别潜在威胁（如：黑客攻击、恶意软件、内部威胁）；

c）识别脆弱性（例如：系统漏洞、配置错误、安全意识不足）；

d）收集历史事件数据（例如：安全事件报告、漏洞扫描结果、渗透测试报告）；

e）审查现有的安全策略、程序和控制措施。

5.2.3 风险分析阶段

a）评估威胁发生的可能性，并分析其对潜在影响；

b）评估脆弱性被利用的可能性，识别潜在的安全风险；

c）评估风险事件对业务的影响（例如：财务损失、声誉损害、法律责任）；

d）根据分析结果确定风险等级。

5.2.4 风险评估阶段

a）基于风险分析结果，确定应对措施并评估现有控制措施的有效性；

b）评估并识别剩余风险，确保对未覆盖风险的充分认识；

c）确定风险的优先级排序。

5.2.5 沟通与报告阶段

a）网络安全服务机构及时与保险人及时沟通初步风险评估结果及结论；

b）保险人结合投保人的保险需求进一步沟通存在问题并征求意见；

c）网络安全服务机构根据反馈调整报告并交付最终风险评估报告。

6 网络安全保险保前风险评估

保前风险评估是保险人在承保前，委托网络安全服务机构对投保人/被保险人进行的全面风险评估与量化分析，旨在确定风险水平，为核保决策（是否承保、承保条件、费率厘定）提供核心依据。评估手段包括网络安全防护自评估及技术探测评估，通常通过问卷评估组织内部安全措施及防护等级，并结合行业属性和保险保障范围等因素，综合量化风险水平。

6.1 评估目标

a）识别并量化投保人/被保险人面临的网络安全风险水平；

b）评估其现有网络安全防护措施的有效性；

c）提供风险加固建议，辅助改善风险状况；

d）为保险人决定是否承保、承保范围、免赔额设定、保险费率厘定提供客观依据。

6.2 评估流程

保险人应主导并按照以下流程开展承保前网络安全保险风险评估工作：

a）评估启动与边界界定

1）基于投保人/被保险人的保险需求，明确本次评估的具体目标；

2）界定评估范围，明确评估覆盖的系统、网络、业务环节、物理位置；

3）基于行业特性及保障需求确定适用的评估标准/问卷模板。

b）风险识别与信息收集

1）综合运用采用风险评估问卷、访谈调研及技术等方法识别评估对象的安全风险；

2）系统性收集信息，覆盖组织架构、管理制度、技术防护、人员意识、供应链管理等各方面。

c）风险分析与量化评分

1）基于收集的信息，按照预先设计的评估模型（包含基础评估和场景评估指标及其权重）进行分析;

2）根据评估项的实际符合程度进行评分;

3）计算整体风险分值及关键场景风险分值;

4）综合分析风险状况，确定风险等级。

d）报告编制与交付

网络安全服务机构应对风险识别与分析结果进行整合，编制正式风险评估报告，报告内容应清晰包含评估概述（目标、范围、方法）、详细风险清单（描述、等级、潜在影响）、风险分值计算过程与结果、明确的风险等级评定、具体可行的风险加固与改进建议、评估结论（对核保的风险提示），并在约定时间内向保险人交付报告。

6.3 评估内容

网络安全风险评估基于已有安全措施进行指标设计并采用结构化指标体系进行量化评分。指标体系设计应基于行业最佳实践、合规要求（如等级保护）并紧密结合保险保障责任。其中，评估指标应包括基础评估指标和风险场景评估指标，具体评估项数可根据业务实际情况进行制定。基础评估标准是评估网络安全的核心内容，通常涵盖网络基础设施安全、数据安全保护、应用程序安全等方面的基本要求，直接反映了被评估对象的网络安全状况是否符合基础建设要求；风险场景评估指标一般用于衡量具体风险场景网络安全风险的大小，可以更好地了解评估对象潜在的威胁和漏洞。具体可参考附录 A 风险评估示例。

6.3.1 基础评估项

基础评估项是评估整体的网络安全防护基础能力，是风险场景抵御能力的前提。基础评估项应结合保险人需求及评估对象的行业属性，从内部安全管理、外部安全防护两方面进行风险识别内容设计，包括但不限于以下几点：

表 1　基础评估项示例

种类	风险识别项	风险识别内容
内部安全管理	网络安全策略与制度	是否实施相应策略和流程以确保遵守网络安全法、行业法律法规或合同要求
	网络安全组织机构	是否设置主管信息安全管理工作的职能部门，并设立系统管理员、网络管理员、审计管理员等岗位和岗位职责
	等保建设	是否按照系统定级组织制定系统安全防护建设方案，并定期组织开展系统的安全等级保护测评与整改工作
	外包商管理	是否将任一部分的网络、计算机系统开发或信 息安全工作委托外包作业
		是否建立了外包商信息安全管理策略（包括但不限于数据使用等管理规范、外包商遴选/管理方式及流程等）
	供应链管理	是否有供应链安全管理制度，并对供应商开展安全调查
		是否与选定的供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务，明确提供者的安全责任并作出必要安全承诺，由于供应商原因导致发生网络安全事件需承担相应赔偿责任
	安全巡检	是否建立对系统进行常态安全巡检的机制，定期进行安全配置检查和安全漏洞扫描，并督促整改和加固
	程序备份	是否备份了适用的驱动程序或应用程序安装文件（与备份， 软件许可协议等一起存储），并定期监测备份功能性
	意识培训	是否每年至少对员工开展一次全员安全意识教育培训
	应急管理	是否制定重要事件的应急预案，包括处理流程等内容
		是否定期对员工进行应急预案演练
外部安全防护	入侵防范	是否关闭了非必要的系统服务和默认共享，且不存在非必要的高危端口（如 445、135、139 等）
		是否有补丁推送更新机制（计算机终端及所有服务器）
	恶意代码防范	是否计算机终端及所有服务器使用防毒保护及程序以防护及阻止病毒、计算机蠕虫、间谍程序及其它恶意程序
	边界安全	是否在重要网络区域与其他网络区域之间（如内外网）部署了网闸、防火墙和设备访问控制列表(ACL)等可靠的技术隔离手段
		是否有独立的虚拟网段用于端到端的加密访问
	安全审计	是否启用安全审计功能，对应用系统所 有用户操作进行审计
		是否定期备份审计日志
	身份访问控制	是否通过堡垒机或防火墙、安全域等对终端接入范围进行限制
		员工账号是否有分类分级
	邮件管理	是否在关键网络节点处部署邮件防护相关产品或技术措施，并配置防范策略
	漏洞管理	是否对发现的安全漏洞及时进行修补或评估可能的影响后进行修补，确保漏洞补丁经过测试后才可使用
	数据保护	是否根据数据的重要性和敏感程度对在信息系统及终端上存储的数据及其介质采取加密、备份等安全保护措施

6.3.2 风险场景评估项

风险场景评估项重点聚焦保险保障中关注的高频、高损风险场景，主要是评估组织的专项防御和应对能力，针对网络勒索、营业中断、数据安全风险场景进行指标细化。

表 2　网络勒索风险场景评估项示例

种类	风险识别项	风险识别内容
内部安全管理	管理制度	是否建立了网络安全勒索情报的收集、处理、管理机制
	意识培训	是否开展了网络勒索防范的专项培训（如网络钓鱼）

	邮件管理	是否实施了基于域的邮件身份验证策略
	应急预案	是否制定了专门针对网络勒索场景的应急响应制度和流程
外部安全防护	入侵防范	是否安装了最新的防病毒和反恶意软件并定期更新
	网络分段	是否采用了网络分段策略，以限制攻击的扩散
	监测预警	是否采取技术措施检测勒索软件及其他恶意软件

表 3 营业中断风险场景评估项示例

种类	风险识别项	风险识别内容
安全管理	供应链管理	是否评估供应链和第三方服务提供商的安全性及连续性计划
	应急预案	是否有针对服务器故障、业务系统故障、重要网络设备故障等场景导致重要业务连续性中断的专项应急预案
外部安全防护	物理安全	是否设置冗余或并行的电力电缆线路为计算机系统供电
	边界防护	是否提供关键边界防护设备的硬件冗余
		是否存在可以直接中断关键业务会话的特征匹配规则

表 4 数据安全风险场景评估项示例

种类	风险识别项	风险识别内容
内部安全管理	管理制度	是否有健全的数据安全管理办法和规范
	定期评估	是否定期开展数据安全风险评估
	数据分级	是否制定数据分类分级策略、方法及制度，并开展数据分级工作
	数据采集	是否在数据采集时按照统一标准及要求，规范数据入库操作
	数据处理	数据导出是否有明确的安全评估和授权审批流程
	数据存储	是否对重要业务信息、系统数据、软件系统等对象具备并维 持本地备份及恢复程序
	数据传输	数据导出是否有明确的安全评估和授权审批流程
	应急预案	是否有针对服务器故障、业务系统故障、重要网络设备故障等场景导致重要业务连续性中断的专项应急预案
外部安全防护	数据处理活动	是否使用安全协议（如 SSL/TLS）对数据进行加密
	数据安全技术	是否采取加密、脱敏、去标识化等技术手段保护重要数据、 敏感数据及个人信息等的安全
	数据审计	是否有针对数据库记录、数据安全产品日志的审计
	数据管理	是否有数据泄露防护产品或数据监测运营平台

6.3.3 风险分值计算

6.3.3.1 计算步骤

风险分值计算分成以下几个步骤：

a）确定评估项及权重：网络安全服务机构与保险人可根据投保人/被保险人的行业特性、业务模式、保障需求共同协商确定基础评估项及场景风险评估项的关键风险识别项的项数及风险识别内容，并结合评估对象的业务属性为每个评估项分配权重。

b）评估项评分：针对每个评估项的子项，根据评估对象的符合程度进行评分。

表 5 单项评估风险评估结果对应分值

风险评估结果	得分
是（达到要求）	子分项满分
部分达到要求	50%×子分项满分
否（未达到要求）	0 分

c）分值汇总计算：将所有评估项的分值根据计算公式进行汇总计算，得出整体风险评估分值。

6.3.3.2 计算公式

整体风险分值（S）计算公式如下：

$$S = (W_{base} \times S_{base}) + \Sigma W_{scenario-i} \times S_{scenario-i}$$

式中：

* S： 整体风险分值（满分 100 分）

* W_{base}：基础评估项权重（建议值 70%）

* S_{base}：基础评估项得分 （满分 100 分）

* $W_{scenario-i}$：第 i 个风险场景评估项权重（所有场景权重之和建议值 30%）

* $S_{scenario-i}$：第 i 个风险场景评估项得分（满分 100 分）

注：

1. 整体风险分值、基础评估项、各单一风险场景评估项的满分分值为 100 分；

2. 建议基础评估项 70%，风险场景评估项权重之和为 30%，可根据具体业务视情况调整；

3. 如保险保障不涉及某单一风险场景，对应$W_{scenario-i}$计为 0

6.4 评估报告

《网络安全保险保前风险评估报告》是核保的关键参考，网络安全服务机构应按既定规则进行风险问卷评估，并视情况进行技术手段探测，最终出具风险评估报告，内容应包括：

a）评估概况：评估目标、范围、时间、依据标准、使用的主要方法（问卷、访谈、工具扫描）、评估团队。

b）评估对象概述：被评估组织基本情况、主要业务、关键信息资产简述。

c）详细风险清单： 按风险等级（高/中/低）或类别列出所有识别出的风险项，清晰描述风险、脆弱性/威胁、潜在的业务影响（及对应的保险损失）及证据来源，并列明针对已发现的高风险领域提出改进建议和风险缓解措施；

e）结果汇总：论述评估对象的网络安全风险概况，汇总评估结果进行最终风险等级确定。

f）改进与加固建议：针对中高风险项，提出具体、可操作、优先级高的改进建议和风险缓释措施。

6.5 风险等级、风险分值与核保决策关系

网络安全服务机构应计算得出评估对象的风险分值给予保险人。保险人进一步结合保险承保影响因素（如评估被保险人的行业属性、法律风险、历史风险发生情况等），决定是否承保，并提供保险报价。其中，风险得分越高，表示企业的安全状况越好，保险费率可能相对较低；反之，风险得分低的企业可能面临更高的保险费率和更严格的条款限制。

表 6 风险等级、风险分值与核保建议的关系

风险分值	风险等级	核保建议	说明
0 ~60 分（含）	高风险	建议不予承保	安全基础薄弱，存在大量高风险项，事故概率及预期损失高。
60~80 分（含）	中风险	建议加固后承保或限额承保	存在显著风险，需明确整改要求，承保后加强过程风控；或通过严格条款控制风险。
80~90 分（含）	较低风险	建议正常承保	安全状况达到基本要求，风险在可控范围内
90~100 分（含）	低等风险	建议优惠承保	安全状况良好，风险管理优秀，可给予费率优惠或更宽松条款。

7 网络安全保险过程风险评估

过程风险评估指在保险期间内，保险人委托网络安全服务机构持续对被保险人网络安全状况进行监测、评估与管理，旨在及时发现新风险、验证控制措施有效性、督促风险改善，从而降低事故发生概率及损失程度，实现风险减量。

7.1 评估目标

过程风险评估旨在通过持续监测影响被保险人风险变化的因素，及时发现新出现的风险因素，并督促评估风险控制措施有效性。

a）持续监控被保险人网络安全风险状况的动态变化；

b）识别保险期间内新出现或变化的风险因素（如系统重大变更、新漏洞利用、新攻击手法）；

c）评估已有风险控制措施（尤其是保前建议措施）的实施效果与有效性；

d）提供持续的风险管理建议，帮助被保险人改善安全态势。

7.2 评估内容及频次

7.2.1 过程风险评估内容

过程风险评估内容应覆盖可能影响被保险人风险状况的关键领域：

a） 内部变更监测：

1） 重大信息系统上线、升级、架构变更；

2） 核心网络拓扑调整；

3）关键安全策略、流程变更；

4）重要供应商/外包商变更；

5）重大组织架构或安全团队变动。

b） 外部威胁监测：

1）与被保险人相关的行业高危漏洞披露；

2）针对被保险人所在行业或使用技术的新型攻击手法（如零日漏洞利用）。

7.2.1 过程风险评估频次

网络安全服务机构需结合被保险人的行业属性及风险等级，针对不同等级的客户应实行定期的、不同频次的过程风险评估及管理标准，确保客户的网络安全得到充分保障，并能及时应对潜在风险。

a）高风险客户

对于高风险客户，需维持较高的服务频次，包括每月进行安全评估，每周监控安全事件，每季度进行员工网络安全风险培训。

b）中风险客户

对于中等风险客户，需维持稳定的服务频次，每季度进行安全评估、每月监控安全事件，每半年进行员工网络安全风险培训。

c）低风险客户

对于低风险客户，可采取较为宽松的服务频次，每半年进行一次安全评估、每季度监控安全事件等，至少进行 1 次员工网络安全风险培训。

7.3 评估工具

经被保险人授权，网络安全服务机构可综合使用以下工具和技术进行过程风险评估：

a）渗透式服务：通过模拟黑客攻击的测试方式来评估系统、网络或应用程序的安全性，以发现系统中存在的潜在安全漏洞，并向客户提供详细的安全建议以改善其安全性；

b）漏洞扫描服务：指利用自动化工具对系统、网络或应用程序进行扫描，以识别可能存在的安全漏洞，并提供漏洞的详细描述以及修复建议；

c）基线核查服务：评估组织的安全基线是否符合最佳实践和标准，并提供改进建议以满足标准要求；

d）威胁情报分析：收集、分析有关潜在威胁、攻击者活动和漏洞信息，了解当前的威胁态势，预测可能的攻击行为，并采取相应的防护措施以应对威胁。

e）行业信息分析：分析特定行业的安全趋势、风险因素和最佳网络安全防御实践，更好地制定适合被保险人业务的安全策略和措施，以提高整体安全水平。

7.4 评估成果

网络安全服务机构应持续实施风险评估，识别被保险人保险标的面临的不断变化的风险和脆弱性，从而降低网络安全风险事件发生的可能性。当保险标的发生重大变更时，应针对重大变更进行风险评估；当发现安全新威胁时，应针对严重程度及对业务的影响程度进行综合分析，并形成相应风险管理建议等服务成果，定期通过邮件或其他约定方式对被保险人进行风险通告或预警，其过程控制的服务成果交付应按规定的关键节点，提交服务成果，包括阶段风险的服务过程报告、总结报告及管理建议；并保证所有服务的交付成果需满足真实性、准确性、完整性和可追溯性。

8 网络安全保险事故风险评估

网络安全事故风险评估是保险事故处理的关键环节。网络安全事故发生后，保险人应联合具备资质的网络安全服务机构，在约定时效内启动标准化事故风险评估，快速厘清事件性及风险溯源，并对被保险人系统恢复状况进行再评估，防范二次风险衍生。

8.1 评估目标

a）事件定性定责：确认事故是否属于保险责任范围;

b）损失精准量化：核算直接经济损失与对被保险人的间接影响。

c）风险溯源归因：分析事故根本原因，为风险调整提供依据。

d）理赔决策支持：出具事故鉴定报告，作为定损理赔的核心凭证。

8.2 评估流程

8.2.1 事故报告与响应启动

a）快速响应：保险人联合网络安全服务机构建立 7x24 小时应急响应团队，在接到事故报告后 1 小时内启动评估程序；

b）信息收集：保险人与网络安全服务机构使用标准化的事故报告模板收集信息；

c）初期控制：在初步信息收集的基础上，网络安全服务机构需为被保险人提供紧急控制建议。

8.2.2 现场调查与证据采集

网络安全服务机构在获得保险人及被保险人的授权后，应及时对报告的网络安全事故进行调查及证据采集，为后续的风险分析提供参考，具体包括如下：

a）技术取证：保全日志记录、系统镜像、网络流量数据等；

b）人员访谈：了解事故发现过程、应急处置措施、业务影响情况等；

c）环境勘察：检查网络架构、安全防护设施、管理制度执行等。

8.2.3 事故溯源与风险评估

a）攻击溯源分析：基于取证数据还原攻击路径，网络安全服务机构需确定入侵方式（漏洞利用、钓鱼邮件等），关联威胁情报定位攻击源，深入分析技术漏洞及管理缺陷等根本原因；

b）二次风险评估：网络安全服务机构需基于评估数据泄露、供应链攻击、监管处罚等衍生风险，出具《持续风险监测方案》，避免二次风险事故发生。

8.3 评估成果

网络安全保险事故风险评估交付物需包括以下两部分：

a）事故评估报告文档（含执行摘要、技术分析报告、损失评估报告、责任认定报告），系统呈现事故时间轴、事故重构、分项量化损失及精算依据、责任归因与保险责任匹配结论；

b）风险管理建议：从技术加固、管理改进、到持续监控（含≥180 天日志留存）形成闭环改进方案，为后续风险防控与保险服务升级提供决策支撑。

附录 A（资料性）

风险评估表示例

风险评估表（满分 100）					
基础评估项 70%	种类（满分分值）	风险识别项（整体分值占比）	风险识别内容	分数区间	是/否/部分达到要求
	内部安全管理（50 分）	网络安全策略与制度（10%）	是否实施相应策略和流程以确保遵守网络安全法、行业法律法规或合同要求	0-5	
		网络安全组织机构（10%）	是否设置主管信息安全管理工作的职能部门，并设立系统管理员、网络管理员、审计管理员等岗位和岗位职责	0-5	
		等保建设（20%）	是否按照系统定级组织制定系统安全防护建设方案，并定期组织开展系统的安全等级保护测评与整改工作	0-10	
		外包商管理（10%）	是否将任一部分的网络、计算机系统开发或信 息安全工作委托外包作业	0-2.5	
			是否建立了外包商信息安全管理策略（包括但不限于数据使用等管理规范、外包商遴选/管理方式及流程等）	0-2.5	
		供应链管理（10%）	是否有供应链安全管理制度，并对供应商开展安全调查	0-2.5	
			是否与选定的供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务，明确提供者的安全责任并作出必要安全承诺，由于供应商原因导致发生网络安全事件需承担相应赔偿责任	0-2.5	
		安全巡检（10%）	是否建立对系统进行常态安全巡检的机制，定期进行安全配置检查和安全漏洞扫描，并督促整改和加固	0-5	
		程序备份（10%）	是否备份了适用的驱动程序或应用程序安装文件（与备份， 软件许可协议等一起存储），并定期监测备份功能性	0-5	
		意识培训（10%）	是否每年至少对员工开展一次全员安全意识教育培训	0-5	
		应急管理（10%）	是否制定重要事件的应急预案，包括处理流程等内容	0-5	
			是否定期对员工进行应急预案演练	0-5	
	外部安全防护（50 分）	入侵防范（20%）	是否关闭了非必要的系统服务和默认共享，且不存在非必要的高危端口（如 445、135、139 等）	0-5	
			是否有补丁推送更新机制（计算机终端及所有服务器）	0-5	
		恶意代码防范（10%）	是否计算机终端及所有服务器使用防毒保护及程序以防护及阻止病毒、计算机蠕虫、间谍程序及其它恶意程序	0-5	
		边界安全（20%）	是否在重要网络区域与其他网络区	0-5	

			域之间（如内外网）部署了网闸、防火墙和设备访问控制列表(ACL)等可靠的技术隔离手段		
			是否有独立的虚拟网段用于端到端的加密访问	0-5	
		安全审计（10%）	是否启用安全审计功能，对应用系统所 有用户操作进行审计	0-2.5	
			是否定期备份审计日志	0-2.5	
		身份访问控制（10%）	是否通过堡垒机或防火墙、安全域等对终端接入范围进行限制	0-2.5	
			员工账号是否有分类分级	0-2.5	
		邮件管理（10%）	是否在关键网络节点处部署邮件防护相关产品或技术措施，并配置防范策略	0-5	
		漏洞管理（10%）	是否对发现的安全漏洞及时进行修补或评估可能的影响后进行修补，确保漏洞补丁经过测试后才可使用	0-5	
		数据保护（10%）	是否根据数据的重要性和敏感程度对在信息系统及终端上存储的数据及其介质采取加密、备份等安全保护措施	0-5	
风险场景评估项30%	**网络勒索风险场景（100 分）**				
	内部安全管理（50 分）	管理制度（10%）	是否建立了网络安全勒索情报的收集、处理、管理机制	0-5	
		意识培训（20%）	是否开展了网络勒索防范的专项培训（如网络钓鱼）	0-10	
		邮件管理（10%）	是否实施了基于域的邮件身份验证策略	0-5	
		应急预案（10%）	是否制定了专门针对网络勒索场景的应急响应制度和流程	0-5	
	外部安全防护（50 分）	入侵防范（20%）	是否安装了最新的防病毒和反恶意软件并定期更新	0-10	
		网络分段（20%）	是否采用了网络分段策略，以限制攻击的扩散	0-10	
		监测预警（10%）	是否采取技术措施检测勒索软件及其他恶意软件	0-5	
	营业中断风险场景（100 分）				
	安全管理（40 分）	供应链管理（20%）	是否评估供应链和第三方服务提供商的安全性及连续性计划	0-20	
		应急预案（20%）	是否有针对服务器故障、业务系统故障、重要网络设备故障等场景导致重要业务连续性中断的专项应急预案	0-20	
	外部安全防护（60 分）	物理安全（30%）	是否设置冗余或并行的电力电缆线路为计算机系统供电	0-30	
		边界防护（30%）	是否提供关键边界防护设备的硬件冗余	0-20	
			是否存在可以直接中断关键业务会话的特征匹配规则	0-10	
	数据安全风险场景（100 分）				
	内部安全管理（60 分）	管理制度（5%）	是否有健全的数据安全管理办法和规范	0-5	
		定期评估（10%）	是否定期开展数据安全风险评估	0-10	
		数据分级（5%）	是否制定数据分类分级策略、方法及制度，并开展数据分级工作	0-5	
		数据采集（10%）	是否在数据采集时按照统一标准及要求，规范数据入库操作	0-10	
		数据处理（10%）	数据导出是否有明确的安全评估和	0-10	

			授权审批流程		
		数据存储（10%）	是否对重要业务信息、系统数据、软件系统等对象具备并维 持本地备份及恢复程序	0-10	
		数据传输（5%）	数据导出是否有明确的安全评估和授权审批流程	0-5	
		应急预案（5%）	是否有针对服务器故障、业务系统故障、重要网络设备故障等场景导致重要业务连续性中断的专项应急预案	0-5	
	外部安全防护（40 分）	数据处理活动（10%）	是否使用安全协议（如 SSL/TLS）对数据进行加密	0-10	
		数据安全技术（10%）	是否采取加密、脱敏、去标识化等技术手段保护重要数据、 敏感数据及个人信息等的安全	0-10	
		数据审计（10%）	是否有针对数据库记录、数据安全产品日志的审计	0-10	
		数据管理（10%）	是否有数据泄露防护产品或数据监测运营平台	0-10	

注：各评估识别项可根据实际情况进行调整。

附录 B（资料性）

网络安全服务机构能力评分示例

保险人可通过设计涵盖企业稳健性、服务经验、团队能力、技术实力四大核心维度的评估体系，并在各维度下设细分子类并采用 0~10 分制量化评分（0 分为极差，10 分为极优），依据预设权重系数加权计算总分（满分 100 分）进行科学筛选。实施过程中需遵循以下规则：

a）评分规则：由评估主体根据服务机构在子类指标中的实际表现独立赋分，评分依据包括资质文件、案例验证及技术测试等客观证据；

b）等级划分：总分≥85 分评定为“优选级合作伙伴”，70~84 分评定为“达标级合作机构”，低于 70 分视为未满足合作基准条件；

c）实施要求：评估方应公开权重分配逻辑，确保评分过程可追溯，结果需经复核确认后生效。

表 B. 网络安全服务机构能力评分表格示例

评价内容	评价指标	评分标准	得分
企业稳健性（权重 30%）	从业时间	企业至少成立 3 年，具备一定的网络安全监测评估能力、应急响应等能力，有明确的发展方向和强大的市场潜力	0-10 分
	营业状况	连续 3 年财务状况、营收盈利能力稳定	0-10 分
	供应链管理	有完善的供应商管理目录，且对同类产品和服务有多个合格供应商	0-10 分
服务经验（权重 30%）	大客户服务数量	至少 10 个大客户服务项目经验（每一大客户服务收入不低于 100 万）	0-10 分
	行业经验	深入多个行业，有至少 5 个不同行业的服务经验和案例积累	0-10 分
	客户留存率	客户续签率不低于 50%	0-10 分
团队能力（权重 20%）	团队专业性	针对网络安全保险服务有对立的项目服务团队，且网项目负责人具备 2 年以上相应网络安全服务项目经验，且内设有 7×24 小时应急处理热线及专业支持团队	0-10 分
	人员素质	服务人员具备 GB/T42446 规定的网络安全服务相关的知识和技能要求,熟练掌握《国家网络安全事件应急预案》网络产品安全漏洞管理规定》等的要求,接受岗前培训并经考核评定合格后上岗，且项目服务人员每年教育培训时长不少于 30 个学时	0-10 分
技术实力（权重 20%）	技术创新能力	拥有的核心技术和创新能力，使用先进的且有效的安全技术，并持续投入科技研发	0-10 分
	项目管理及服务能力	具有完备的项目管理、安全保密管理、质量管理等规章制度，并符合相关项目监管规定，能提供广泛、深入、高度定制化的安全解决方案以满足不同客户需求	0-10 分

参考文献

[1] GB/T 20985.1/2《信息技术 安全技术 信息安全事件管理 第 1 部分：事件管理原理/第 2 部 分：事件响应规划和准备指南》
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/Z 24364—2009 信息安全技术 信息安全风险管理指南
[4] GB/T 25069—2022 信息安全技术 术语
[5] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
[6] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
[7] GB/T 36635—2018 信息安全技术 网络安全监测基本要求与实施指南
[8] GB/T 36687—2018 保险术语
[9] GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南
[10] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[11] NIST SP 800-30 风险评估指南
[12] ISO/IEC27005 信息安全风险管理框架