ICS 35.240.01
I6440

团　体　标　准

T/WHCSA007-2024

网络安全风险量化评估规范

Specification for Quantitative Assessment of Cybersecurity Risks

2024-12-30 发布　　2025-01-10 实施

武汉市网络安全协会 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由牵头单位武汉华康科技有限公司联合上海竟安网络科技有限公司提出并归口。

本文件起草单位：武汉华康科技有限公司、上海竟安网络科技有限公司、广东电信规划设计院、武汉市网络安全协会、湖北公众信息产业有限责任公司、国家工业信息安全发展研究中心、中南财经政法大学金融研究院、江汉大学人工智能学院、湖北大学网络空间安全学院、国家计算机网络应急技术处理协调中心湖北分中心、国任财产保险股份有限公司、中国平安财产保险股份有限公司湖北分公司、中国人民财产保险股份有限公司武汉分公司、中国联合网络通信有限公司湖北省分公司、长江财产保险股份有限公司、武汉东湖科技保险发展促进中心、湖北省电子信息产品质量监督检验院、武汉路特斯科技有限公司、上海东航数字科技有限公司、湖北天融信网络安全技术有限公司、北京长亭科技有限公司、湖北连邦云创科技有限公司、武汉明嘉信技术有限公司、武汉安经纬业信息安全技术有限公司

本文件主要起草人：周韬、吉贻俊、王菱犀、刘悦恒、乔奇、马航、黄培欣、金飞、吴婷、孙倩文、丁雨晗、徐晟、邓宏涛、何鹏、彭骏、王媛、胡湄伊、林千帆、丁瑞、韩直新、冯军、吴仁杰、彭湃、熊吉、周丹、东明、曾峥、艾龙、王晓明、杨永刚、王丽波、李智、孙智、张玉萍、严媛

引　言

在数字经济浪潮汹涌澎湃的今天，网络安全不仅是组织稳固基石，更是其持续发展与创新的坚强后盾。面对日益复杂多变的网络威胁环境，制定一套科学严谨、全面系统的《网络安全风险量化评估规范》标准显得尤为关键。本标准旨在通过精确的风险量化评估，为组织筑起一道坚实的网络安全防线。

网络攻击者不断采用先进技术手段，利用外部暴露面和内部管理漏洞作为突破口，严重威胁着组织的数据安全、服务连续性和业务稳定性等。为了有效应对这些挑战，本标准不仅提供了详尽的风险识别框架，还融入了量化评估方法，确保组织能够准确把握风险全貌，制定针对性的防范策略。

通过实施《网络安全风险量化评估规范标准》，有助于组织构建起一套高效运行的网络安全管理体系，实现从风险识别、量化评估到风险应对的全程监控与管理。这不仅能够提升组织对网络安全风险的感知能力和应对能力，还能为组织的数字化转型和业务发展提供坚实的安全保障。

网络安全风险量化评估规范

1 范围

本文件给出了网络安全风险量化评估术语定义、实施原则、评估思路、评估内容、周期、步骤和结果应用等规范方法的指引。

本文件适用于各类组织，包括但不限于企业、政府机构、非营利组织等。包括组织网络安全风险量化评估管理、数字供应链安全管理、网络安全保险评估及合规与审计支持等应用场景，可以根据组织的特定情境进行灵活应用，以满足不同行业及场景的独特需求。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

武汉市网络安全评价参考指标体系

信息安全风险处理实施指南 GB/T33132-2016 信息安全技术

GB/T20984-2022 信息安全技术信息安全风险评估方法

ISO/IEC27001 系列

NISTCybersecurityFramework

GB/T25069-2022 信息安全技术术语

GB/T36637-2018 信息安全技术 ICT 供应链安全风险管理指南

GB/T32921-2016 信息安全技术信息安全技术信息技术产品供应方行为安全准则

COBIT 框架等。

3 术语定义

《武汉市网络安全评价参考指标体系》中界定的术语和定义适用于本文件。为了便于使用，以下重复列出了某些术语和定义，并对文件中出现的其它术语进行定义。

3.1 风险评估

风险评估是一个系统性过程，旨在识别、分析和评估组织面临的潜在安全风险。

3.2 网络安全风险量化评估

网络安全风险量化评估是使用定量方法（如概率模型、统计分析等）来评估数字资产（如计算机系统、数据、网络等）面临的威胁和风险水平。这种方法通过具体的数据和指标，提供对潜在安全风险的量化描述，以支持决策者制定有效的风险管理策略。

3.3 组织安全量化指数

组织安全量化指数是一个综合指标，用于衡量组织整体安全态势的强弱。该指数通常基于各种安全因素和事件（如安全漏洞、攻击次数、合规情况等），通过量化的方法来评估组织的安全防护能力和有效性。

3.4 内部安全管理量化指数

内部安全管理量化指数是针对组织内部安全管理措施和实践的量化评估指标。它衡量组织内部的安全管理水平，包括政策执行、员工培训、访问控制等方面，以反映内部安全管理的强度和效果。

3.5 外部安全有效性量化指数

外部安全有效性量化指数是用于评估组织在对外合作或面对外部威胁时的安全防护有效性的指标。这包括对组织暴露面、外部泄露数据、第三方供应商、合作伙伴及外部环境的安全防护能力的量化分析，以确保组织在外部环境中的安全性。

3.6 组织量化评级

组织量化评级是对组织整体安全状态进行数值化评价与评级的过程。这种评级通常基于具体的量化数据和标准，将安全性能转化为可比较的数值或等级，以便于分析和决策。

3.7 组织暴露面

组织暴露面指的是组织在网络安全环境中暴露给潜在威胁和攻击的所有入口点和暴露的区域。这包括硬件、软件、网络接口、员工行为、暴露数据、下属机构、第三方供应链等所有可能被攻击者利用的点。

3.8 下属机构

下属机构是指一个组织下级的各类分支机构或子公司。这些机构通常需要遵循主组织的安全策略和标准，以确保整个组织的安全一致性和有效性。

3.9 外部数据泄露

外部数据泄露指的是组织数据在未经授权的情况下被第三方访问、获取或公开的事件。这类泄露通常涉及来自外部攻击者、合作伙伴或供应链中的漏洞，可能导致敏感信息被暴露，从而引发法律、财务及声誉上的严重后果。

3.10 第三方供应链

第三方供应链是指与组织合作的外部供应商、服务提供商和合作伙伴。这些第三方可能提供产品、服务或系统，其安全性和可靠性直接影响到组织的安全防护。

3.11 网络安全保险

网络安全保险是一种保险产品，旨在为组织提供在发生网络安全事件（如数据泄露、网络攻击等）时的财务保护。它覆盖的内容可能包括数据恢复费用、法律费用、罚款、赔偿责任等，以帮助组织减轻因安全事件带来的经济损失。

4 风险量化评估概述

4.1 评估原则

4.1.1 一致性原则

风险量化评估在不同组织与系统间保持高度的统一性和规范性，确保评估结果的可比性与标准化。通过明确和统一的度量指标、评估方法和分析框架，实现不同系统与机构间的有效对比和协调。建立标准化的评估流程，保障所有参与方在统一基准上执行风险评估，以产出一致、可靠的评估报告，进而促进跨部门及跨组织的顺畅沟通与合作。

4.1.2 实用性原则

风险量化评估应体现实际应用价值，有效助力组织识别与管理网络安全风险。以操作性为导向，提供明确、可执行的评估流程与具体控制措施，确保在网络安全管理中得到切实应用。通过明确的评估方法及可行的风险应对策略，助力组织精准识别潜在威胁，科学评估风险程度，进而制定针对性防护措施，优化风险管理效率，强化网络安全防护能力。

4.1.3 动态适应性原则

风险量化评估展现卓越的适应力，灵活应对威胁环境与技术进步，确保评估的实时性、准确性与持续性。面对网络安全威胁与技术的不断演进，建立更新与调整机制，紧跟最新风险态势与防护需求。集成实时数据与信息反馈，及时优化评估方法与参数，保持风险评估结果与当前安全形势的高度契合，为组织提供精准的风险识别与高效应对策略。

4.2 评估思路

网络安全风险量化评估由两部分组成，分别为技术角度的外部安全量化评估和管理角度的内部安全量化评估。其中技术角度的外部安全量化评估建议常态化进行，通过自动化工具和系统来实现；管理角度的内部安全量化评估工作频率则应结合政府工作计划及组织的风险承受能力、业务性质和外部环境变化进行合理设定。

4.3 评估度量

在组织网络安全风险量化评估时，按照总分100分的原则，将评分结果分为四个等级：A、B、C、D。每个等级对应一个具体的分数区间，通过结合以下两种方法来确定最终的综合量化安全分数：

a）技术侧外部安全自动化评估：采用标准的自动化工具对系统进行评估，智能得出量化的安全分数。

b）管理侧内部数据分析评估：根据管理层指定的特定评估指标来收集和分析数据，得出量化的安全分数。

具体分数区间如下：

a）A档：90＜分数≤100分

b）B档：75＜分数≤90分

c）C档：60＜分数≤75分

d）D档：0＜分数≤60分

4.4 风险量化等级划分

通过明确定义的评估等级，标识组织级别安全风险的严重性。等级划分应基于风险的可能性和影响，确保评估结果的权威性和可比性。

a）等级A-低风险：风险的可能性和影响较小，可能对组织的安全性产生轻微的影响。应对该等级的风险采取基本的安全措施。

b）等级B-中风险：风险的可能性和影响属于一般范围，可能对组织的安全性产生一定的影响。需要采取适度的风险缓解措施。

c）等级C-高风险：风险较高，可能性和影响较大，可能对组织的安全性产生严重影响。需要采取紧急的风险缓解措施。

d）等级D-临界风险：风险极高，可能性和影响非常大，可能对组织的安全性产生灾难性的影响。需要立即采取紧急的、全面的风险缓解措施，并进行紧急响应。

等级的定义和标准可根据组织的具体情况和业务需求进行调整及定制。评估时，根据风险的特征和严重程度，将其划分到对应的等级，并确保这些等级在整个组织中得到了一致的理解和接受。

5 评估内容

评估内容引用自武汉市网络安全评价参考指标体系。

根据国家有关政策及法律法规要求，结合各行业特点和当年度工作重点规划，确定安全量化指数评估重点，实施过程中，组织可根据需要调整安全量化指标和评分规则。指标权重的取值通过专家分析并结合年度工作重点综合确定。评估指标如图1所示。

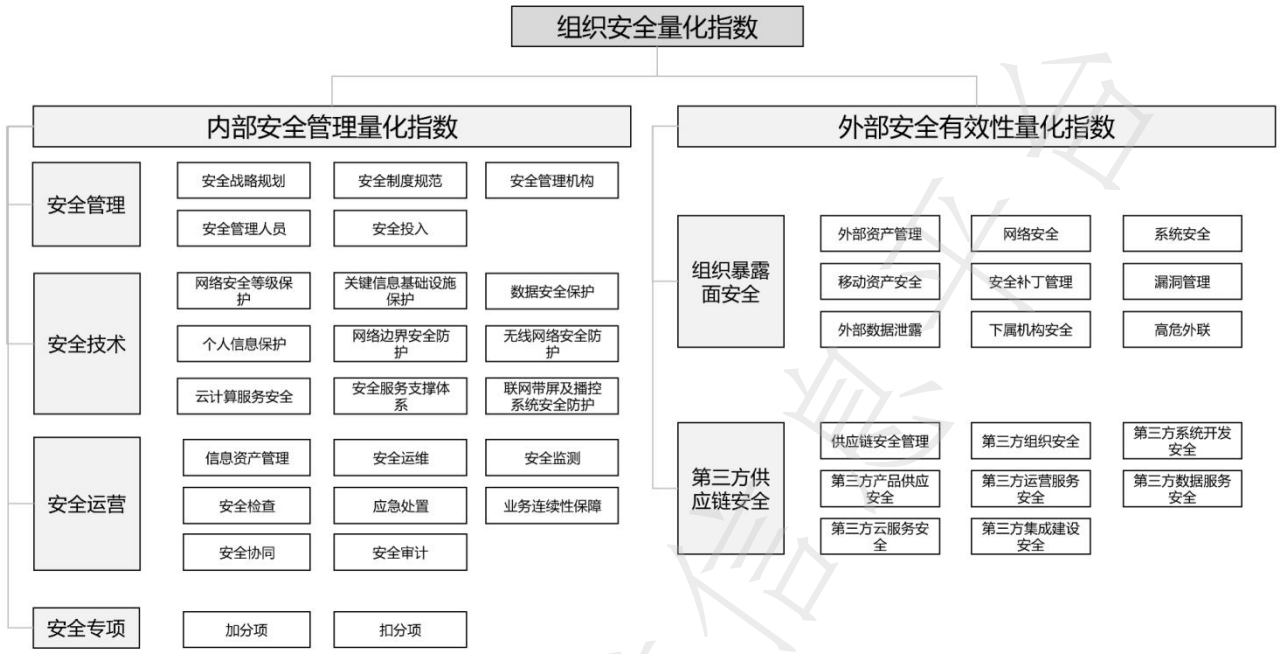

图 1 组织安全量化指数

6 评估周期

安全量化评估涵盖内部与外部两大维度。外部层面的安全量化评估应常态化，依托自动化工具与系统高效执行；内部层面的安全量化评估频率则需依据政府工作规划、组织风险承受力、业务特性及外部环境变迁综合考量后合理设定。特别在以下情况下，建议定期进行评估：

a）重大变化时评估：如业务扩展、系统升级、新增关键应用等。

b）事件驱动评估：发生重大安全事件或漏洞曝光后立即进行。

c）法规变化时评估：当法律法规或行业合规要求发生变化时，及时调整评估策略。

7 评估流程

7.1 流程概述

网络安全风险量化评估流程，主要包括评估准备、评估方案编制、评估数据采集、评估数据分析、评估报告编制五个阶段。

7.2 评估准备

7.2.1 明确评估目标

网络安全风险量化评估的主要目的是使用定量方法来评估组织面临的威胁和风险水平。通过具体的数据和指标，提供对潜在安全风险的量化描述，为决策者提供科学高效的风险管理决策依据，引导组织加强网络安全防护体系建设，提升整体网络安全防护水平和风险应对能力。

7.2.2 确定评估范围

根据工作需要和评估目标，确定网络安全风险量化评估的对象、范围和边界，明确评估涉及的管理文档、记录表单、数据资产、业务和信息系统、人员、供应商、暴露面等。其中组织暴露面包括硬件、软件、网络接口、员工行为、暴露数据、下属机构、第三方供应链等所有可能被攻击者利用的切入点。

7.2.3 组建评估队伍

根据评估范围、涉及的行业特征、专业需求，选择具备相关专业能力的评估人员组成评估队伍。评估人员应进行评估技术培训和保密教育，并签订保密协议。评估队伍在检查评估中获取的信息，只能用于检查任务目的。

7.3 评估方案编制

7.3.1 确定评估指标和权重

根据国家有关政策及法律法规要求，结合各行业特点和当年度工作重点规划，确定安全量化评估重点，根据需要调整安全量化评估指标和指标权重。一级指标和二级指标的权重取值主要由领导根据当前工作重点确定。

表1给出了指标权重的样例。

表1　单位机构网络安全量化指数指标权重

一级指标	安全管理			安全技术			安全运营			组织暴露面安全			第三方供应链安全		
一级指标权重	w_1			w_2			w_3			w_4			w_5		
二级指标	安全战略规划	安全制度规范	……	网络安全等级保护	关键信息基础设施保护	……	安全运维	安全监测	……	外部资产管理	网络安全	……	供应链安全管理	第三方组织基础安全能力	……
二级指标权重	$w_{1,1}$	$w_{1,2}$		$w_{2,1,}$	$w_{2,2}$		$w_{3,1}$	$w_{3,2}$		$w_{4,1}$	$w_{4,2}$		$w_{5,1}$	$w_{5,2}$	

7.3.2 制定评估计划

建立可行性的评估计划，明确具体时间进度安排和人员安排。确保评估时间安排与业务运营和关键项目的时间相协调，以最大程度减少对业务运营的影响。

7.3.3 建立风险应对措施

依据国家及地方相关法律法规和国家标准，针对网络安全风险量化评估过程中可能面临的挑战与潜在风险，识别数据安全与网络安全等关键风险点，制定相应的风险管理措施，明确风险预防与控制策略。

7.3.4 形成评估工作方案

评估工作方案应基于评估准备情况编制，内容包括但不限于评估背景、评估目标、评估范围、评估重点、评估指标、数据采集方案、评估工作队伍、评估计划、风险应对措施等。

7.4 评估数据采集

7.4.1 内部安全管理量化指数

根据指标评估要求，采集所需的数据和资料。数据采集来自多个渠道，以确保全面性和可靠性，包括组织内部系统（如信息安全监控系统、操作日志、财务记录等），这些系统提供了直接、实时的风险相关数据；外部信息（如行业标准、安全报告、法规要求等），这些可以补充和验证内部数据；组织反馈（如问卷调查、面谈记录等），这有助于获取对风险的主观评估和实际问题的直接反映。综合多种数据来源可以全面了解组织的风险状况，减少数据盲点和偏差。

数据采集方法包括具体的手段和步骤，用于获取和记录所需的评估数据。明确数据采集需求和数据来源，选择适宜的数据采集方法。一般数据采集方法包括资料审阅、问卷调查和系统取数等。此外，定期更新和维护数据采集计划是必要的，以确保数据的时效性和准确性。数据清理也是关键步骤，它涉及去除重复记录、处理缺失值等，以提高数据的质量。在数据采集过程中，还需要考虑数据保护措施，确保数据的安全性和完整性。

7.4.2 外部安全有效性量化指数

通过主动扫描工具结合被动信息收集，发现组织所拥有的互联网暴露面数字资产，并将其分为不同的类别，以建立数字资产的清晰框架，每一个资产类别都会进行详细的记录和定期更新，为后续的风险评估和管理提供基础数据支持，确保评估的全面性和准确性。

外部暴露面资产指的是一个组织、系统或应用程序在互联网上对外开放、可被访问的部分。它包括所有可能与外部网络或用户进行交互的接口、服务、端点和资源，主要包含但不限于公共IP地址空间、开放端口、Web服务、外部接口、远程访问服务、高危外联、云服务及第三方服务平台等。外部暴露面资产范围包括组织主体自身、下属控股机构、外泄敏感数据及重要第三方供应链组织。

7.5 评估数据分析量化

7.5.1 内部数据分析与量化评估

数据分析旨在运用统计工具与分析方法，对收集的数据进行深度剖析，从而洞察风险模式与趋势。此过程核心在于采纳诸如风险矩阵、概率-影响图等分析模型，实现对数据风险因素的量化评估与深入理解。同时，借助统计分析与回归分析等技术手段，精准识别数据中的关键变动趋势及潜在风险点，为决策提供坚实的数据支撑。

量化评估过程旨在将分析结果转化为具体的风险量化数值，以便于进行统一的评估与比较。此过程涉及为各项指标科学分配权重，并基于详尽的数据分析结果，综合计算出管理侧内部安全管理量化指数的具体评分。进而，通过风险优先级的科学排序，为组织明确指出需优先应对的风险领域，确保资源的有效配置与风险管理的精准施策。

管理侧内部安全量化指数计算方式可参考附录A。

7.5.2 外部数据分析与量化评估

组织应依据自身需求，精心选取适宜的风险量化手段，包括但不限于定性评估、定量分析以及蒙特卡洛模拟等方法，并从多维度进行深入分析与实施。从以下几个方面展开：

a）数据聚合与清洗：通过整合多种数据源，包括但不限于漏洞、情报、资产、威胁、行为及结果等，采用高效的数据清洗算法剔除噪声数据，精简冗余信息，以确保数据的精准度与完整性。此过程涵盖丢失数据处理、数据异常修复及数据格式规范化，旨在构建高质量的数据基础。

b）机器学习和统计模型：采用预测分析技术，结合机器学习算法深度剖析历史数据，精准识别并预测潜在的安全威胁与趋势。

c）风险评分算法：针对多样化数据与指标，实施加权评分机制，以精准衡量其对整体安全性的影响力。具体而言，依据安全事件、漏洞及配置错误的严重程度，分配差异化权重。运用加权平均算法，量化各风险因素对综合评分的贡献度，确保高风险因素（如严重漏洞）获得更显著的影响权重。此外，为捕捉安全态势的动态演变，引入时间衰减模型，逐步降低过往事件对当前评分的影响，从而保证评分体系能够更为精准地映射当前安全状态。

技术侧外部安全量化指数计算方式可参考附录B。

7.6 评估报告编制

评估报告编制是根据评估结果和评估过程反映出的情况，深入分析组织安全量化指数，形成评估报告。评估队伍依据评估工作方案、各类指标得分、各级指标得分以及评估结果分析情况等，编制评估报告。

评估报告分为管理侧内部安全量化评级报告和外部安全风险量化评级报告。

a) 管理侧内部安全量化评级报告核心聚焦于风险量化评估流程与成果的精炼呈现，全面涵盖概览、关键发现、数据分析及建议策略四大板块。报告开篇即阐明评估背景、对象与方法论，随后直指评估中凸显的主要风险点及其数据支撑。进一步，深入剖析数据，量化展示风险评分与趋势走向。报告尾声，则提出一系列针对性强、操作性高的改进建议与行动计划，旨在指导组织精准应对识别风险，强化内部安全管理机制，确保策略与步骤的有效实施。

b) 外部安全风险量化评级报告结构严谨，涵盖封面、目录、引言、方法论、暴露面与风险识别、量化评估、结果分析、建议与缓解措施、附录及总结结论等关键章节。引言简明扼要地阐述报告背景、目的与范围；方法论章节明确说明采用的评估手段与风险量化模型。随后，报告详细识别并列举系统攻击面、潜在威胁与漏洞，通过量化模型精准分析风险概率与影响，并以风险矩阵直观呈现风险优先级。最终章节汇总核心发现，提出具体可行的改进建议与缓解策略，并附上详尽数据与文档资料，为风险管理策略的制定奠定坚实基础。此结构化报告设计旨在高效传达评估成果，促进风险管理决策的科学性与有效性。

评估报告可参考附录C报告格式。

8 评估结果应用

8.1 组织安全量化管理

在组织的安全量化管理体系中，网络安全风险量化评估构成了系统化识别与评估潜在安全威胁的基石，确保组织能够精确把握安全态势及风险暴露。此评估机制通过量化手段，使组织能够清晰洞察每项安全风险的可能性与潜在后果，进而依托数据支撑，精准制定安全策略与防护措施，实现资源优化配置与整体防护效能的显著提升。此数据驱动的管理模式，不仅强化了决策过程的科学性，还极大地促进了风险管理效率与成效的飞跃。

8.2 政府安全合规管理赋能

在政府网络安全监督与管理领域，网络安全风险量化评估为政策制定与监管工作奠定了坚实的数据基础。该手段聚焦于关键基础设施与重点行业的量化分析，助力政府精准识别并优先处理重大网络安全风险，据此制定高效且具有针对性的政策与监管举措。借助数据驱动手段，政府机构得以全面洞悉国家网络安全状况，促进资源优化配置，提升监管效率与效能，同时强化整体网络安全防御能力。

此外，政府通过实施标准化的风险量化评估规范，强化安全合规管理，为监管机构配备了高效工具。此举确保了各组织安全评估的公平性与客观性，精准识别安全短板，并驱动组织及时整改。此过程不仅构建了统一的安全基准，还促进了行业安全水平的整体提升，为监管机构提供了坚实的决策依据，有力推动了行业的稳健与可持续发展。

8.3 数字供应链安全管理

随着供应链数字化转型的加速，组织应高度重视数字供应链安全风险管理，保障与供应链合作伙伴间的数据与网络安全。通过量化评估供应链各环节风险，组织可精准识别并应对潜在安全弱点，制定有效防护措施，预防供应链漏洞引发的安全事件。同时，网络安全量化评估促进供应链上下游统一安全标准，增强整体安全韧性及抗风险能力，保障业务连续性与稳定性。结合组织安全量化管理方法，系统化识别评估安全威胁，精确把握安全态势与风险暴露，优化资源配置，提升整体防护效能，实现数据驱动决策与高效风险管理。

8.4 网络安全保险

网络安全风险量化评估在网络安全保险中发挥着至关重要的作用，它通过精确量化潜在安全事件的概率与影响，为保险公司提供详尽的风险暴露与潜在损失数据，显著提升保险服务的精准度与产品的针对性、有效性。此举助力保险公司设计更合理的保障方案，精准定价，并确立科学、准确的赔付标准。同时，它引导组织清晰认知自身风险敞口，合理选择保险覆盖范围，并接受具体风险改善建议，实施精准风险管理，有效降低网络风险损失，激发投保积极性，增强整体安全防护能力，共同推动网络安全保险市场的稳健发展。

9 后续工作

9.1 风险处置和复评

被评估方需制定整改方案，并设定明确时限予以实施。若遇整改延期，应立即实施临时性安全保障措施，以规避网络安全风险。整改完成后，评估队伍将视情况启动网络安全风险量化评估复评流程，复评重点聚焦于风险处置后的残余风险分析，以及评估额外控制举措可能引发的次生风险影响。

9.2 持续监控和评估结果更新

持续监控与评估结果更新是保障网络安全风险量化评估效能的核心举措。定期组织审查，能迅速捕捉新兴安全威胁与风险演变，促进安全策略与防护措施的即时调整。构建长效监控体系，紧跟安全态势演变，确保评估结果精准映射现实环境。此外，量化评估模型与数据需定期迭代，纳入最新网络安全威胁与技术动态，以强化风险评估的时效性与准确性。此动态优化机制赋能组织对风险保持高度敏锐，提升网络安全防护的灵活性与防御效能。

9.3 评估工作改进和优化

网络安全风险量化评估的精确与效率提升是评估工作改进与优化的核心目标。组织应实施定期审查，优化评估手段与工具，涵盖模型调整、数据采集技术更新及流程精简。依托结果反馈与效果分析，精准定位并解决瓶颈问题，持续精进评估品质。同时，融合前沿技术如机器学习与数据分析，深化评估精准度与洞察力。持续推动评估工作的迭代升级，维护其科学性与实效性，有效应对网络安全威胁的日新月异。

10 其它

10.1 工具和技术推荐

10.1.1 安全评估工具

推荐采用官方认可的安全量化评级工具，以优化网络安全评估效能。此类工具需获评估对象正式授权，通过自动化量化技术，精准输出详尽的安全评分报告，为评估对象提供全面的网络安全状况洞察。工具能持续监控评估对象的公开网络资产，评估配置安全性，识别外部脆弱性，并融合威胁情报分析，深入剖析

外部暴露面，追溯历史安全事件，同时监控并评估组织的公开信誉状况。综合多维度评估结果，生成科学、全面的安全数据集，为决策制定与风险管理提供坚实支撑。

10.1.2 数据采集和分析技术

通过综合风险量化评估与管理系统，结合数据采集和分析技术，可以有效整合和解读数据，为组织提供更有效的安全量化评估结果，为决策提供有力支持。

数据采集技术包括在线问卷调查平台，自动化分发工具，数据导入与整合等。

分析技术则涵盖统计分析、数据可视化、数据挖掘、文本分析和趋势分析等，帮助识别数据中的模式和趋势。

10.2 培训和认证

10.2.1 培训计划

建立网络安全风险量化评估团队的培训计划，使团队成员了解网络安全风险量化评估的基本概念和方法，提升团队成员在实际应用中的技能，包括风险识别、评估、量化和管理，确保团队成员熟悉相关的标准和规范，以及在评估过程中遵循的最佳实践。培训内容可以包括但不限于：

a）风险管理基础：掌握风险管理的基本理论和流程，包括风险识别、评估、响应和监控。

b）风险量化评估方法：学习定性与定量风险评估方法，风险评分模型及评估概率和影响的技术。

c）数据收集和分析：了解数据收集来源、分析技巧以及如何从数据中提取有价值的信息。

d）报告和沟通：掌握撰写风险评估报告的技巧，以及如何向非技术人员有效沟通评估结果。

e）实践演练：通过案例分析和模拟演练，增强实际应用中的技能和问题解决能力。

f）工具和技术：介绍常用风险评估工具和软件，并学习其配置和使用技巧。

10.2.2 认证计划

为确保网络安全风险量化评估团队的专业胜任能力，所有成员应持有如CISP等国家认证的网络安全资质。此类认证彰显了成员在风险管理及信息安全领域的深厚理论基础与实践能力。认证培训需涵盖理论学习、考试准备，并实施定期更新机制，以维持团队成员专业知识的先进性与时效性。

此外，应构建认证记录档案，以追踪成员认证的有效期限及继续教育进展。实施定期认证评估，确保团队全体成员持续符合业界标准，进而提升评估工作的质量水准与可靠性。

10.3 评估机构与人员认定和管理

10.3.1 评估机构认定

数字安全量化评级服务商（以下简称量化评估机构），作为经本标准发布机构或经本标准发布机构授权的分支机构按照本条款评估合格，可以依据本标准开展评估认定工作，该机构必须对本标准有深刻的理解具备开展评估工作的必要软硬件实力，评估团队应接受本标准的相关培训，持有相关认证、丰富的网络安全经验和专业团队，并坚守独立性与透明度原则，以保障评估过程和结果的公正、可信。

a) 评估机构申请：申请成为本标准量化评估机构需获本标准发布机构的正式授权，并持有网络安全评估相关资质。机构认定授权表可参见附录D。

b) 系统服务能力：从事本标准规范的量化评估机构需拥有成熟的量化服务产品与系统能力，提供高效、精准的评估平台，且该能力需经本标准发布机构定期检验和评价。

c) 专业积淀：从事本标准规范的量化评估机构应积累丰富的网络安全评估经验，组建具备CISP等认证的专业团队。

d) 独立透明原则：量化评估机构应确保独立运作，避免利益冲突，同时保证评估过程与结果的透明度，便于评估对象及利益相关方理解。

10.3.2 人员认定和管理

为确保评估流程的有效执行与结果的可信度，对量化评估机构及其人员的严格认定与管理至关重要。通过设定高标准的资质要求、丰富的实践经验以及持续的专业培训，确保评估团队具备卓越的专业能力，为组织提供坚实的安全评估保障。

a) 团队构建：多元化专业背景

评估团队汇聚了网络安全专家、资深系统管理员及合规性顾问等多领域人才，确保评估工作的全面覆盖与深入洞察。

b) 专业培训与资质认证：强化专业能力

团队成员定期参与专业培训，紧跟网络安全领域最新动态。同时，积极鼓励并支持团队成员获取如CISP等专业认证，以不断提升专业素养。

c) 保密协议：严守信息安全

所有团队成员均签署保密协议，严格遵守信息安全规定，确保评估过程中发现的敏感信息得到有效保护，防止未经授权的泄露。

d) 高效沟通与精准报告：助力决策制定

团队成员具备卓越的沟通与报告能力，能够清晰、准确地传达评估结果与建议，为组织高层管理者及技术团队提供有力的决策支持。

附录A
（规范性）
内部安全量化指数计算方法

（1）三级指标测评得分确定：

第i个一级指标的第j个二级指标的第k个三级指标$U_{i,j,k}$，其评估结果$S_{i,j,k}\in\{0,0.4,0.7,1\}$，其中1表示符合，0表示不符合，0.4和0.7表示部分符合。部分符合分为两种场景，当$U_{i,j,k}$的分值0＜评价标准＜0.5时，分值为0.4；当$U_{i,j,k}$的分值0.5≤评价标准＜1，分值为0.7。

（2）二级指标测评得分确定：

第i个一级指标的第j个二级指标$S_{i,j}$为该二级指标内所有$n_{i,j}$个三级指标测评结果的算术平均值（四舍五入，取小数点后2位），即：

$$S_{i,j}=\frac{\sum_{1\le k\le n_{i,j}} S_{i,j,k}}{n_{i,j}}$$

（3）一级指标测评得分确定：

每个二级指标会根据相关政策赋予权重$w_{i,j}$，第i个一级指标L_i的量化评估结果S_i为该一级指标内n_i个二级指标测评结果$S_{i,j}$的加权平均值（四舍五入，取小数点后2位），即：

$$S_i=\frac{\sum_{1\le j\le n_i} W_{i,j}S_{i,j}}{\sum_{1\le j\le n_i} W_{i,j}}$$

（4）整体管理侧内部安全量化指数得分：

每个一级指标都被分配相应的权重w_i，量化评估结果S 为所有n个一级指标测评结果S_i的加权平均值（四舍五入，取小数点后2位），再加上专项安全的加减分总数X，即：

$$S=\frac{\sum_{1\le i\le n} W_i \cdot S_i}{\sum_{1\le j\le n} W_i}\times 60+X$$

附录B
（规范性）
外部安全量化指数计算方法

外部安全量化评级通过使用数据驱动、由外而内的方法对组织的安全有效性进行评分。通过检查外部可观察安全配置情况,并根据以下指标进行分别评分：

D={

IP信誉度情况,
面向互联网公共服务暴露情况,
面向互联网的高危外联情况，
域名与DNS安全情况,
网络服务配置安全性情况,
应用服务配置安全性情况,
补丁周期情况,
漏洞响应与修复效率情况,
漏洞管理报告与监控落实情况,
.....
}

每个指标的得分使用专有算法f每日计算得出,评分公式如下：

Sd（类别评分）=*f*(asset，issue，duration)

其中评分算法考虑因素以下：

asset（数字资产的数量和类型）：通过互联网空间测绘等技术观察到的组织的数字资产情况。

issue（问题级别和数量）：数字资产外部可观察到的安全配置的问题情况。

duration（事件持续时间）：计算首次观察到数字资产与最后一次看到数字资产之间的时间。

综合的安全评分是针对该组织标准化的所有指标评分（具有不同权重 W）的汇总结果。

Ts（总分）=Σi∈DSdi*Wi

附录C
（规范性）
安全量化评级报告

一、管理侧内部安全量化评级报告

1. 评估概况
   - 评估背景
   - 评估对象
   - 评估原则
   - 评估过程
   - 数据采集
2. 评估结果
   - 总体情况
   - 工作成效和存在问题
3. 安全管理指数
   - 总体分析
   - 分指数分析
4. 安全技术指数
   - 总体分析
   - 分指数分析
5. 安全运营指数
   - 总体分析
   - 分指数分析
6. 安全专项指数
   - 总体分析
   - 分指数分析
7. 工作建议
   - 安全评级的历史趋势
   - 最新安全挑战和变化

二、外部安全风险量化评级报告

1. 量化评级介绍
   - 目的和背景
   - 评级方法论概述
   - 评级结果的使用和目标
2. 等级划分
   - 安全风险等级定义
   - 各等级对应的安全措施建议
3. 评估维度
4. 安全总览
   - 组织信息
   - 资产信息
5. 量化评级分数与概括
   - 各维度得分和权重分配
   - 安全风险总体评级
   - 关键风险点概述
6. 行业对标
   - 行业标准与实践比较
   - 竞争对手安全实践概况
7. 量化趋势
   - 安全评级的历史趋势
   - 最新安全挑战和变化
8. 各领域评级概览及建议措施
9. 风险清单
   - 漏洞详细列表与风险级别
   - 恶意活动的发现与分类
10. 问题清单
    - 发现的问题与漏洞
    - 需要进一步评估和解决的安全挑战

附录：

- 评级方法细节与工具使用说明
- 术语表和缩写定义

此外，报告的格式应包括清晰的标题和子标题、图表和表格的使用以支持数据可视化，以及每个章节的详细内容展开，以便清楚地呈现评级结果和建议措施。

附录D

（规范性）

数字安全量化评级服务商认定表

数字安全量化评级服务商授权申请表

认证机构信息

- 认证机构名称：（本标准发布机构：武汉市网络安全协会）
- 认证机构的资质和背景介绍：

服务商信息

- 公司名称：
- 注册地址：
- 联系人姓名：
- 联系电话：
- 电子邮件：
- 网站链接：

1.公司背景与资质

- 成立时间：
- 注册资本：
- 公司规模（员工数量）：
- 相关行业认证（如ISO27001等）：
- 服务历史与客户范围：

2.评估方法与技术

- 使用的评估方法论：
- 评估工具和技术：
- 评估覆盖的安全领域：
- 评估结果的报告形式和内容：

3.专业资质与员工能力

- 安全评估相关的专业资质和认证：
- 员工培训与持续教育计划：
- 技术团队的专业领域和经验：

4.法律合规与隐私保护

- 符合的法律法规和行业标准：
- 客户数据保护和隐私政策：
- 数据处理和存储地点：

5.安全管理与客户支持

- 安全管理体系与流程描述：
- 客户支持服务（包括响应时间、支持方式等）：

6.参考客户及案例

- 参考客户名称及行业：
- 相关成功案例或客户见证：