ICS号
中国标准文献分类号

团　体　标　准

团体标准编号
代替的团体标准编号

网络安全风险量化评估规范

Specificationforquantitativeassessmentofcyber securityrisks

Xxxx-xx-xx发布xxxx-xx-xx实施

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xxxxxxxxxxxxxxxxxxxxxxxx提出并归口。
本文件起草单位：xxxxxxxxxxxxxxxx。
本文件主要起草人：xxxxxxxxxxxxxxxxx

引　言

在数字经济时代，组织日益依赖于数字化技术进行业务运营，信息技术系统的复杂性和互联性逐渐增加，网络安全威胁与风险随之扩大。网络攻击者采用先进的技术手段，通过外部暴露面和内部管理的技术漏洞入侵系统，导致数字组织数据泄露、服务中断以及其他严重后果。为了帮助组织更好地理解和管理这些风险，本文件旨在提供一个全面的网络安全风险量化评估管理标准及实施指南。

网络安全风险量化评估规范

1 范围

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，无论其规模和行业。适用范围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。规范中的方法和指南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。本规范通过提供一套标准化、系统化的风险量化评估框架，旨在帮助各类组织提升网络安全防护能力和风险管理水平。

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。

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

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 术语和定义

下列术语和定义适用于本文件。

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 目的

本文件的主要目的是提供一套标准化和系统化的方法，以量化评估和管理组织的网络安全风险。通过统一的评估指标和方法，不同组织能够在本规范的指导下进行风险量化评估，从而确保评估结果的客观性、可比性和一致性。该规范结合系统化的技术量化评估与安全管理评估过程，有助于提高组织内部对网络安全风险的认知，并为决策者提供科学高效的风险管理决策依据。此外，本规范还旨在促进信息共享与合作，从而增强整个行业在网络安全领域的整体抵御能力。

5 量化评估原则

5.1 网络安全风险量化的重要性

网络安全风险量化有助于组织全面理解和管理网络安全挑战，针对性提高安全水平，降低事故发生概率及影响。在国家、行业和企业层面，网络安全风险量化推动安全度量透明管理，建立可视化可信赖的安全机制，促进信息共享与合作，维护生态系统的安全稳定。其重要性体现在以下方面：

a)精准评估风险程度：量化风险帮助组织准确评估潜在风险的严重性及损失，便于有针对性地采取防护措施。

b)资源优先级确定：通过风险量化，组织可优化安全资源分配，集中解决最关键和风险最高的领域，提升防护效果。

c)支持决策制定：风险量化提供数据支持，帮助决策者理解安全问题并制定合适的应对策略。

d)资源有效利用：量化风险优化安全资源高效配置，减少投入与风险之间的不平衡。

5.2 原则

a)一致性原则：

风险量化评估在不同组织和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和标准化。通过明确并统一评估方法、度量指标和分析框架，实现不同系统和机构间的有效对比和协调；设立标准化的评估程序，确保各参与方能够在相同的基础上进行风险评估，从而提供一致且可靠的评估结果，支持跨部门及跨组织的沟通与合作。

b)实用性原则：

风险量化评估应具备切实的应用价值，便于有效识别和管理组织内的网络安全风险。以操作性为导向，提供清晰且可执行的评估步骤和具体的控制措施，使其能够在实际的网络安全管理中得到应用；通过明确的评估方法和实际可行的风险应对策略，帮助组织识别潜在威胁并评估其风险程度，从而制定合理的防护措施，提升风险管理效率和网络安全防护能力。

c)动态适应性原则：

风险量化评估具备灵活的调整能力，以应对不断变化的威胁环境和技术进步，从而确保评估的实时性、准确性和持续性。随着网络安全威胁和技术的持续演变，应具备更新和调整的机制，以反映最新的风险状况和防护需求；同时能够集成实时数据和反馈信息，及时优化评估方法和参数，确保风险评估结果与当前安全态势保持高度相关，提供有效的风险识别和应对方案。

6 指标与度量

6.1 安全评估指标体系

评估指标应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。

图 1 网络安全量化指标

6.2 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。

6.3 评估度量

在组织网络安全风险量化评估时，按照总分 1000 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：900＜分数≤1000 分

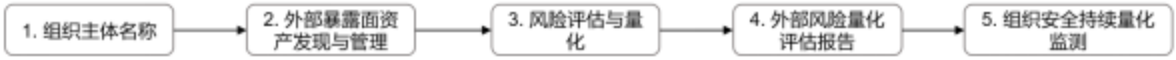
b）B 档：750＜分数≤900 分

c）C 档：600＜分数≤750 分

d）D 档：0＜分数≤600 分

7 组织主体名称

7.1 外部安全有效性量化指数



7.1.1 组织主体名称

风险量化评估基于组织主体进行，通过组织的主体名称，进行后续一系列风险量化评估过程。

7.1.2 外部暴露面资产发现与管理

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、云服务及第三方服务平台等。

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。

7.1.3 风险评估与量化

评估指标包括但不限于外部资产管理、下属机构安全、外部数据泄露、供应链安全管理、第三方组织基础安全能力等。

风险评估可从如下角度来展开：网络设备、系统及应用配置须符合最佳安全实践；数据保护措施有效性验证；需具备威胁感知与应对能力；IP 未被列入信誉度黑名单；DNS 和 SSL 配置安全；邮件服务器配置无漏洞；安全补丁及时管理；防止恶意软件传播；员工具备高安全意识；关注历史安全事件等。

组织可以选择适合组织的风险量化方法，如定性评估、定量分析、蒙特卡洛模拟等。评估算法可参考附录 A，从以下几个方面展开：

a）数据聚合与清洗：通过聚合各类数据，如漏洞、情报、资产、威胁、行为、结果等，利用数据清洗算法处理噪声数据，消除冗余信息，并确保数据的准确性和完整性，包括处理丢失的数据、修复数据异常以及规范化数据格式。

b）机器学习和统计模型：通过预测分析，利用机器学习算法分析历史数据，识别潜在的安全威胁和趋势。

c）风险评分算法：对不同类型的数据和指标进行加权和评分，以反映其对整体安全的影响程度。例如，不同的安全事件、漏洞和配置错误可能被赋予不同的权重。针对每个风险因素，使用加权平均算法计算其对整体评分的贡献，以确保严重的漏洞等因素比轻微的配置错误有更大的影响。为了反映安全状态的动态变化，可能使用时间衰减模型，使较早发生的事件对当前评分的影响逐渐减小，以确保评分更加准确地反映当前的安全状况。

7.1.4 外部风险量化评估报告

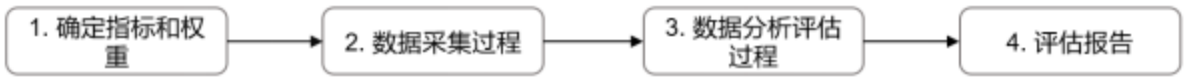
外部风险量化评估报告，需要遵循一个标准化的结构以确保报告的全面性和有效性。报告通常包括封面、目录、引言、方法论、暴露面识别、风险识别、风险量化评估、结果、建议和缓解措施、附录、总结和结论、以及签署和审阅部分。引言部分提供报告的背景、目标和范围；方法论部分描述使用的评估方法和风险量化模型；攻击面识别和风险识别部分详尽列出系统中的攻击面、潜在威胁和漏洞；风险评估部分则通过量化模型分析风险的概率和影响，并通过风险矩阵展示风险优先级。最终，报告总结主要发现，提出改进建议和缓解措施，并附上相关的数据和文档以供参考。这种结构化的报告不仅有助于清晰传达风险评估结果，还为制定有效的风险管理策略提供了基础。

7.1.5 组织安全持续量化监测

组织外部威胁环境和内部业务进程处于不断发展的状态，所面临的风险也相应的不断变化。通过风险

量化持续监测可以实时收集、分析和评估所面临的风险，了解当前安全态势和风险变化。对数据进行深度分析和趋势识别，得出清晰可懂的数据驱动的评估结果，为安全管理提供科学性的优先级建议，最优化资源投资和利用。

7.2 管理侧内部安全量化指数



7.2.1 确定指标和权重

指标选择是组织风险量化评估的基础步骤，这些指标需要能够有效反映组织内部安全的风险状况。具体关键指标的确认需要根据组织的业务特点、面临的安全威胁以及行业标准综合选择。确保所选指标能够全面而准确地捕捉到风险的核心要素，并且具有较好的数据可获得性和度量性。

权重分配是将选定的风险指标按其重要性和影响程度赋予不同权重的过程。通过对各指标在总体风险中所占的重要性进行评估，确定其在总风险评估中的贡献度。权重分配通常基于专业意见、历史数据分析、实际业务需求和行业机构管理计划，以确保评估结果的科学性和准确性。

评估指标选项和权重分配可参考指标体系文件。

7.2.2 数据采集过程

评估数据采集是组织风险量化评估的基础工作，主要根据指标评估要求，采集所需的数据和资料。数据通常来自多个渠道，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；以及组织反馈（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。

7.2.3 数据分析量化评估过程

数据分析是通过应用统计工具和分析方法，对收集到的数据进行深入审查，以揭示风险模式和趋势。这一过程包括运用各种分析模型，如风险矩阵和概率-影响图，来量化和理解数据中的风险因素。通过统计分析、回归分析等方法，识别数据中的关键趋势和潜在的风险点。

量化评估是将分析结果转化为具体的风险量化值，便于进行综合评估和比较的过程。通过为每项指标分配权重，结合数据分析的结果，计算出管理侧安全量化指数的综合评分，并通过风险优先级排序，帮助组织明确应优先处理的风险。

管理侧安全量化指数计算方式可参考附录 B。

7.2.4 评估报告

报告内容是对风险量化评估过程及结果的详细阐述，涵盖了评估的整体概述、主要发现、数据分析结果和建议措施。报告首先介绍评估的背景、对象和方法，然后列出评估中发现的主要风险点和问题，并提供具体的数据支持。接着，详细展示数据分析和量化评估的结果，包括风险评分和趋势分析。最后，报告提出改进建议和具体的行动计划，帮助组织针对识别出的风险点制定有效的应对策略和实施步骤，以增强内部安全管理。

报告呈现是指将评估报告以易于理解和传达的方式进行展示。报告应确保内容清晰简洁，避免使用复杂的术语或冗长的描述，以便管理层和相关人员能够快速把握核心信息。利用图表、图形和数据可视化工具，可以直观展示数据分析结果和风险评分，使信息更加明了。报告的格式和结构应逻辑清晰，通常包括摘要、主要发现、分析结果、建议措施和附录等部分。

8 评估报告

8.1 报告格式

安全量化评估报告分为外部安全量化和内部安全量化，外部安全通过系统化方法来评估风险，针对外部资产安全性进行动态、持续性量化评估；内部安全管理量化评估通过数据收集和专家分析和量化方法，根据实际工作需要来制定评估报告。可参考附录 C 报告格式。

8.2 结果解释

为确保评估结果的准确性、公正性和权威性，评估报告需得到相关行业协会的盖章认可。这一步骤不仅是对报告质量的保证，也是对评估方法是否符合标准规范做最终确认。

8.3 行动计划

建议网络安全量化评估的结果与绩效考核挂钩，并制定对应的长期安全策略来进一步提高安全水平，并将安全优化项列入后续预算和安全规划中。具体来说，将评估结果作为组织安全水平绩效考核的依据，确保相关组织和人员对安全改进负责；调整预算以优先支持重大安全漏洞修复、配置优化和培训等。

9 量化评估实施指南

9.1 评估周期

9.1.1 确定评估频率

安全量化评估由两部分组成，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。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。

9.1.2 制定评估计划

建议建立周期性的评估计划，明确每次评估的计划和截止日期。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。

9.2 工具和技术推荐

9.2.1 安全评估工具

可使用安全量化评级工具来提升网络安全评估的效果，使用这类工具建议得到评估对象授权认可。通过这类工具自动量化技术提供详细的安全量化评分，帮助评估对象全面了解自身的网络安全状况。该类工具可持续监测评估对象公开的网络资产，评估其配置安全，识别其外部脆弱性，并分析威胁情报，同时能深入了解外部暴露面、追踪历史安全事件，并掌握组织的公开信誉。通过以上综合维度评估，获得科学全面的安全数据，助力决策制定和风险管理。

9.2.2 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。

9.3 培训和认证

9.3.1 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。

9.3.2 认证计划

为确保网络安全风险量化评估团队具备必要的专业能力，团队成员应获得如 CISP 等国内认可的网络安全认证。这些认证验证了成员在风险管理和信息安全领域具备扎实的理论基础和实践指导，认证培训应包括理论学习和考试准备，同时需定期更新以保持专业知识的前沿性。

此外，应建立认证记录档案，跟踪成员认证的有效性和继续教育情况。定期评估认证情况，确保所有成员持续符合行业标准，从而提升评估工作的质量和可靠性。

9.4 评估机构与人员认定和管理

9.4.1 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）作为协会、工委会等组织认定的授权评估机构，必须拥有相关认证、丰富的网络安全经验和专业团队，同时保持独立性和透明度，以确保评估过程和结果的公正性和可信度。

a）机构认定：量化评估机构应获得协会或工委会的明确授权认可，并具备相关的网络安全评估资质。机构认定授权表可参见附录 D。

b）系统化能力：量化评估机构需具备相应量化服务产品和系统化能力，可提供高质量、时效性的评估平台，相应能力需得到武汉市网安协会的认证认可。

c）经验与专业知识：评估机构应具备丰富的网络安全评估经验，并有专业的安全团队，包括具备 CISP 等认证的专业人员。

d）独立性与透明度：评估机构应保持独立性，避免与被评估组织存在利益冲突。评估过程和结果应该具有透明度，能够被评估组织和利益相关方理解。

9.4.2 人员认定和管理

量化评估机构和人员的认定和管理是保证评估过程有效性和可信度的关键因素。通过合适的资质、经验和培训，确保评估团队具备足够的专业水平，能够为组织提供有力的安全评估服务。

a）评估团队组成：评估团队应包括具备不同专业领域知识的成员，如网络安全专家、系统管理员、合规性专家等。

b）培训与认证：团队成员应接受定期的培训，保持对最新网络安全威胁和技术的了解。相关认证如 CISP 等应该得到鼓励和支持。

c）保密性要求：团队成员应遵守保密协议，确保评估过程中发现的安全问题不被泄露给未经授权的人员。

d）沟通与报告能力：团队成员应具备清晰的沟通和报告能力，能够向组织高层管理层以及技术团队传达评估结果和建议。

10.应用与改进

10.1 评估结果应用

10.1.1 组织安全量化管理

在组织安全量化管理中，网络安全风险量化评估提供了一种系统化的方法来识别和评估潜在的安全威胁，帮助组织精准理解其安全态势和风险暴露。通过量化评估，组织可清晰地了解每个安全风险的可能性和潜在影响，从而制定基于数据的安全策略和防护措施，有效优化资源配置和提升整体安全防护水平。这种数据驱动的管理方式不仅增强了决策的科学性，还提高了风险管理的效率和效果。

10.1.2 数字供应链安全管理

随着供应链数字化程度的提高，组织必须重视数字供应链安全风险管理，以确保其与供应链合作伙伴之间的数据和网络安全。通过量化评估供应链各环节的安全风险，组织能够识别和针对潜在的安全弱点，制定有效的防护措施，防止供应链漏洞导致的安全事件。此外，网络安全量化评估还帮助供应链上下游组织建立统一的安全标准，从而提升整个供应链的安全性和抗风险能力，确保业务的连续性和稳定性。结合组织安全量化管理方法，组织可以系统化地识别和评估潜在的安全威胁，精准理解其安全态势和风险暴露，优化资源配置并提升整体安全防护水平，从而实现数据驱动的决策和高效的风险管理。

10.1.3 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，通过对潜在网络安全事件的概率和影响进行精确量化评估，为保险公司提供详细的风险暴露和潜在损失数据，不仅提高了保险服务的精准性，还增强了保险产品的针对性和有效性。使保险公司能够制定更合理的保险保障方案，能够更准确地确定保险定价，能够进行科学、合理、准确的赔付标准，同时，帮助组织了解自身的风险敞口，以选择合适的保险覆盖范围，为组织提供具体的风险改善建议，有针对性地开展风险管理，从而减少组织网络风险损失，提升组织的投保积极性和整体网络安全防护能力，促进网络安全保险市场的健康发展。

10.1.4 政府安全合规管理赋能

在政府网络安全监督与管理中，网络安全风险量化评估为政策制定和监管提供了至关重要的数据支持。通过对关键基础设施和行业进行量化评估，政府能够准确识别并优先处理最严重的网络安全风险，制定有针对性的政策和监管措施。量化评估的数据驱动方法使政府机构能够更全面地了解国家网络安全态势，从而合理配置资源，提升监管效能，并增强整体网络安全防御能力。

此外，政府安全合规管理赋能通过标准化的风险量化评估规范，为监管机构提供了有效工具，确保对不同组织进行公平、客观的安全评估，识别安全薄弱环节，并促使组织整改。这不仅建立了统一的安全标准，还提升了行业安全水平，并为监管机构提供了科学的决策支持，推动行业的持续健康发展。

10.2 监控和更新评估结果

监控和更新评估结果是确保网络安全风险量化评估持续有效的关键步骤。定期监控评估结果可以帮助组织及时识别新出现的安全威胁和风险变化，从而迅速调整安全策略和防护措施。组织应建立持续的监控机制，跟踪安全态势的动态变化，确保评估结果与实际情况保持一致。同时，需定期更新量化评估模型和数据，以反映最新的网络安全威胁和技术进展。通过这种动态更新和监控，组织可以保持对风险的及时响应能力，增强网络安全防护的适应性和有效性。

10.3 评估工作改进和优化

评估工作改进和优化旨在提升网络安全风险量化评估的精确性和效率。组织应定期审查和优化评估方法和工具，包括评估模型的调整、数据收集技术的更新以及评估流程的改进。通过收集反馈和分析评估结

果的实际效果，识别并解决存在的问题，可以不断提升评估质量。此外，引入先进的技术和最佳实践，如机器学习和数据分析，能够进一步增强评估的准确性和深度。定期进行评估工作改进，有助于保持评估过程的科学性和有效性，确保组织能够应对不断变化的网络安全威胁。

附录A
（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,
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）=∑i∈DSdi*Wi

附录B
（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＜考核标准＜0.5时，分值为0.4；当$U_{i,j,k}$的分值0.5≤考核标准＜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：

$$S=\frac{\sum_{1\le i\le n} W_i \cdot S_i}{\sum_{1\le j\le n} W_i}\times 600+X$$

附录C
（规范性）
安全量化评级报告

一、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。

二、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

附录D

（规范性）

数字安全量化评级服务商认定表

武汉市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：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：