ISSN：3078-8994
EISSN：3104-4492

基于演练实践的等级保护测评指标适应性优化研究

王宇博　文瑞阳　佘瑾南　佘帅彦

联通数字科技有限公司系统集成事业部，北京 100032

摘　要：随着信息技术的迅猛发展，等级保护测评指标在实际应用中逐渐暴露出与新兴技术和安全需求不匹配的问题。为提高测评体系的适应性与有效性，本文提出基于演练实践的动态调整机制、构建全面灵活的测评指标体系以及利用先进技术提升指标的自动化和智能化等优化对策。通过演练反馈与技术手段的结合，测评指标得以不断完善，能够更好地应对复杂多变的安全威胁，推动信息系统安全管理水平的提升。本文为改进现有测评体系提供了可行的理论依据与实践指导。

关键词：等级保护；测评指标；演练实践；适应性优化

0. 引言

信息安全已成为各行各业发展的基础保障，等级保护是我国信息安全管理的核心措施，大量用于各类信息系统的安全分析，伴随技术的持续进步，传统的等级保护测评指标出现了与实际安全需求不符的情况，致使后果比较难全面体现目前信息系统的安全状况[1]。为此优化现有测评指标体系，增进适应性，已是信息安全方面亟待解决的关键问题，本文依据演练实践，探究优化测评指标的对策，意在为信息系统安全给予更有效、合理的帮助。

1. 等级保护测评指标在信息安全中的重要性

1.1 等级保护制度对信息安全保障的作用

等级保护制度是国家信息安全管理的重要框架，建立了分类分级为基础的安全保障体系，凭借划分不同信息系统的安全级别，制定针对性的保护措施，让各类信息系统根据重要性跟安全需求获得对应保护，该制度明确了信息系统的保护目标跟技术要求，保证系统面对各类网络攻击和内部威胁时可以有效防御，最大限度地保障数据的机密性、完整性以及可用性。等级保护制度助推各类企业以及组织增强信息安全意识，起到了主动作用，伴随网络威胁环境越来越繁复，等级保护的实行给各级政府跟企业给出了统一的安全保障框架，是国家信息安全战略中的重要部分[2]。

1.2 测评指标对等级保护执行效果的影响

等级保护测评指标的设计和执行直接决定了制度执行的效果，测评指标是一种量化手段，能全面折射信息系统实行等级保护时采取的安全措施是否达标，判断能否有效防范潜在安全威胁，凭借合理设计的测评，可对信息系统的安全性实行判断，帮助相关人员采取适当的补救办法。一个准确且严谨的测评指标体系，不只帮助了解信息系统的安全状况，还能针对薄弱环节给出详细精进建议，保证系统长期稳定运作，测评指标体系助推标准化以及规范化的作用十分突出，借助一致的标准，所有系统都能在相同框架下实行衡量，减少了企业跟组织在信息安全防护中的随意性与不规范做法。

1.3 演练实践在评估和优化中的意义

演练实践是一种常见的优化工具，可以加强等级保护测评指标的适应性，借助模拟不同网络攻击场景和安全威胁，可以发现现有测评指标应接现实问题的能力及实际应用中的短板，演练可以测试防火墙、入侵检测系统、数据备份等技术措施应接冗杂攻击时的效果，同样检验现有测评指标是否能真实折射防护措施的实际水平。借助演练反馈优化指标体系，有益于加强动态环境中的适应能力，保证面对新威胁跟技术变化时依旧可靠，演练实践有利于各方理解并使用测评指标，增进了信息安全管理人员执行保障措施的能力，助推持续改良与优化。

2. 当前等级保护测评指标存在的问题

2.1 测评指标与实际安全需求脱节

目前等级保护测评体系设计初期以静态标准为重点，面向传统信息系统的安全需求，伴随云计算、大数据、人工智能及物联网等新型技术的推广，信息系统结构跟运行方式已产生深度改变，实践中测评指标体系依然沿用传统静态安全控制内容，不容易准确折射现代繁复系统的真实风险。云环境下的资源动态调度、虚拟化安全隔离、跨域数据访问等关键问题没能借助现有指标全面体现，测评结果与系统实际防护水平出现偏差，部分指标仅关注设备配置以及制度文件，忽略了系统运行期间的安全状况跟威胁应对能力，结论不容易体现真实的风险情况[3]。

测评实行时，关注点更多放在“是否符合

ISSN：3078-8994
EISSN：3104-4492

标准”，而非“是否具备安全能力”，这一种逻辑让安全管理工作偏向文档审查跟形式化合规，忽略动态风险识别和应急响应能力的重视，实际安全需求一般源于多样化的业务场景与快速变化的攻击手段，测评指标依旧围绕静态控制点展开，比较难全面折射安全策略跟技术防护的灵活性。这致使信息系统凭借检测后依旧隐藏潜在风险，安全管理能力跟风险控制成效没能同步加强，减少了等级保护制度的执行效果与可信程度。

2.2 指标评估方法的局限性

目前的等级保护测评方法侧重定性判断，靠着人工审查、现场访谈跟资料核验等手段得出融合结论，这样的方式在初期阶段有一定的参考价值，但伴随信息系统规模扩展跟威胁环境变得复杂，短板逐渐暴露，人工判断容易因人员经验不同、主观想法以及现场条件限制而缺乏客观性。部分量化环节缺少一致标准，难以完成不同系统间的横向对比跟纵向精进跟踪，特别是面对高复杂度网络架构、混合云部署以及动态业务场景时，传统方式不容易准确折射系统运行的安全特性。

另一种突出问题体现在实时性欠缺，现行测评流程多依赖分段检查，周期内的安全变动比较难及时表现，网络攻击的频率与形式越来越丰富，安全状态有着明显的动态特点，而固定评估无法包含上述变动，由于缺少数据驱动的自动检测方式，部分测评依然需靠着人工，致使效率低下且更新延迟。即便某些系统已引入安全监测跟态势感知技术，数据成果仍未被有效纳入测评框架，致使信息分散、验证链不完整，测评结果的时效性跟可重复性均受限制，不容易助力持续安全改良与指标优化工作的推进 [4]。

2.3 测评指标的更新和适应性问题

等级保护测评指标体系建立时，靠着的是较为稳固的信息安全模型与管理框架，但信息技术发展迅速，新威胁以及新技术接连涌现，让原有体系显得不够及时，一些指标没能紧跟新型技术架构的安全特点，比如云原生安全、数据安全治理、人工智能模型防护等领域缺少对应的标准。测评指标更新周期偏长，修订工作需要多部门配合跟标准审批，实际使用时容易出现标准滞后于技术发展的情形，不同领域的组织为满足特殊需求，常自行补充或改动指标，损害了体系的统一性与可比性。

适应性不足不光体现在指标内容滞后，还表现在指标应用的灵活性不够，测评体系多用统一模板，比较难依据行业特点、系统规模跟业务属性实现差异化精进，一些新兴行业，像智能制造、医疗物联网等，重点安全需求与传统信息系统差异明显，但测评指标依旧偏重通用标准，缺少详细针对性。结果致使测评流程过于死板，结果缺乏实际参考价值，指标更新机制缺少反馈助推跟实践检验环节，使得新指标在实行前不容易判断其成效以及可操作性，更新环节多依赖专家讨论而非实际数据支撑，减少了指标体系的灵活性与预见性。

3. 优化等级保护测评指标的对策

3.1 基于演练实践的动态调整机制

等级保护测评指标体系的优化需以演练实践为依据，建立灵活改良机制，演练是信息安全管理中的核心方法，不光能验证现有安全措施的效果，又能在模拟真实威胁场景下检验以及反馈测评指标的适用性跟精进程度，凭借定期跟不定期的演练活动，可以实时获取各种攻击方式和漏洞信息，融合系统应接演练时的表现，对测评指标实行有针对性的修改以及优化。演练期间，发现的安全漏洞与防护不足可以直接助推测评指标体系的动态精进，保证其跟上新出现的威胁和技术变化，这一类动态优化机制不只靠着演练结果的汇总，还需借助反馈流程跟数据解析方法，形成演练成效与指标精进的闭环联系。模拟勒索病毒攻击演练期间，若部分测评指标无法妥善应对这类攻击形式，演练报告会直接点明这些短板，相关部门分析后会尽快精进指标框架，把新型攻击形式加入测评范围，借助反复演练、反馈、发现问题、优化指标，再实行演练，建立持续改良测评指标的机制，保证其能贴合信息系统实际安全考验 [5]。

动态调整机制的重点亮点是灵活性跟适应性，演练时参与方可以围绕不同场景展开全面测试，包含攻击模拟、漏洞扫描、恢复能力测试等多个维度，这有益于深度了解现有测评指标应对冗杂安全形势的能力，每次演练积累的数据与经验，都会为优化指标体系给予重要参照。这一种机制有利于把安全测评从一次性、静态的检查转为持续、动态的流程，更好应接信息安全领域的变化跟考验，演练实践的加入可以助推各方理解并使用测评指标，参与者能直接体会到指标背后的实际意义和操作要求，加强对测评标准跟技术措施的认可度与执行能力。演练不光增强了测评指标的可操作性，还加深了各类安全管理人员对安全防护的理解，更深一步优化了测评指标的实际效果，借助演练实践的不断完善，等级保护测评体系能更好地适应现实中越来越变化的安全需求。

3.2 构建更加全面和灵活的测评指标体系

伴随信息技术持续进步，单一测评指标不容易应接多样化与复杂化的安全需求，建立更全面、灵活的测评指标体系变得十分重要，全面的测评指标体系应多角度体现信息系统安全

ISSN：3078-8994
EISSN：3104-4492

状况，包含数据保护、身份认证、访问控制、应用安全、网络防护等内容。该体系应具备很强的灵活性，可以依据不同行业、业务需求和系统环境实行定制，保证测评结果准确且适用，为达成这一目标，需先重新审视跟归类现有测评指标，保证包含所有信息安全重点部分，云计算以及大数据环境下，传统安全控制指标不容易应接虚拟化、跨域访问以及数据共享等新考验，所以需要根据上述技术特点设计专门的衡量标准。行业特有的安全需求同样是建立灵活指标体系的重要部分，金融、医疗、教育等不同领域的信息系统，需依照独有的业务和安全需求，量身制定对应的测评标准，保证指标包含行业特有的风险与安全考验。

灵活性是优化测评指标体系的另一个核心要素，信息系统的安全需求伴随技术进步跟业务开拓不停变化，原有的标准化指标大多不容易跟上此类变化，所以建立灵活的指标体系，需要依据不同安全环境的变化及时更新以及修改指标。灵活性体现在三个方面：一是依照系统的规模、类型和安全等级，使用不同的方法跟标准，二是在多云架构、混合网络等新型技术环境下，可以贴合这些技术特点，给出对应的指标；三是借助实时监测跟自动化安全管理工具，优化方针与标准，保证测评指标契合目前环境的安全需要。全面且灵活的测评指标体系可以有效应对不同层次、不同领域的安全考验，为信息系统给予准确的安全分析，凭借持续改良和优化，可以大幅加强测评指标的适应性，保证快速变化的技术环境下始终保持高效的安全分析能力。

3.3 利用先进技术提升指标的自动化和智能化

伴随信息技术快速发展，传统手工操作的测评方法不容易满足信息安全的繁复需求，自动化跟智能化测评工具变成增强测评指标效能的好办法，自动化技术可以高效完成数据收集、分析以及报告生成等任务，减少人工过程中的错误与遗漏，增加结果的准确性以及统一性。凭借引入大数据分析、机器学习等先进技术，可以快速发现潜在安全隐患，优化指标体系，增进安全判断的准确性，自动化工具不只能加快测评速度，还能扩大测评范围，凭借自动化的漏洞扫描、网络流量分析和系统配置检查，可以快速找到信息系统中的安全漏洞跟配置错误。相比传统手动方式，自动化手段缩短了时间，加强了能力，且无需人工加入，减少了失误跟偏差，自动化工具可以完成跨平台与跨环境的检测，保证信息系统在各类冗杂条件下获得一致结果，增强检测精准度与公正性。

智能化技术在自动化基础上，增添了数据深度学习与风险预测能力，机器学习以及人工智能技术可以依据历史数据完成模式识别，自动察觉潜在安全威胁，给出针对性改良方向，借助机器学习算法，系统可参照历史攻击数据推测出现的攻击形式，优化评测标准，保证应对新型攻击的能力。智能化技术可以依据实时监测数据，灵活改变测评标准，贴合信息系统的变化，依据网络行为分析的智能系统，可以自动判断异常流量、非授权访问等威胁，同样反馈测评指标是否符合目前安全状况，借助自动化与智能化技术，等级保护测评指标的执行能力以及质量有望大幅增进。信息系统的安全状况会更加准确跟全面，不光增强了检测的合理性和准确性，还让检测结果更具实用性跟参考价值，技术一直发展后，检测体系将更智能、更贴合需求，能更好适应各类信息安全要求。

4. 结论

本文详细剖析了目前等级保护测评指标遇到的关键问题，提出了借助演练实践精进动态机制、打造全面且灵活的测评指标体系以及借助先进技术增强自动化跟智能化水平的优化方法，实行此类方法后，不只能增加测评指标的适应能力，还能更有效地应对新兴技术引发的安全考验。伴随信息安全威胁的持续变化，优化测评体系能助力信息系统的安全保障，增进国家和企业的防护能力。

参考文献：

[1] 李志文 , 梁承东 . 基于贝叶斯网络的等级保护测评辅助方法 [J]. 电子质量 , 2024(2):12-15.

[2] 漆桃 . 等级保护测评过程中的风险控制 [J]. 软件 , 2024, 45(4):110-112.

[3] 顾碧波 , 钱磊 . 网络安全等级保护测评中网络安全现场测评方法 [J]. 计算机产品与流通 , 2024(8):158-160.

[4] 贺承玮 , 陈柯序 . 网络安全等级保护测评中网络安全现场测评方法 [J]. 网络安全技术与应用 , 2024(1):12-14.

[5] 马力 . 网络安全等级保护测评中测评结论的度量方法优化 [J]. 信息网络安全 , 2020(5):10-12.

作者简介：王宇博，（2000.9—），男，汉族，河南，本科，测评师，研究方向：信息安全。