

引用格式: 李永刚, 林亮成, 韩淞. 电力企业网络安全测评冗余治理: 机制创新与标准化实践[J]. 标准化学报, 2026(10): 122-128.
LI Yonggang, LIN Liangcheng, HAN Song. Redundancy Governance in Cybersecurity Compliance Inspections of Power Enterprises: Mechanism Innovation and Standardization Practice[J]. Journal of Standardization, 2026(10): 122-128.

电力企业网络安全测评冗余治理: 机制创新与标准化实践

李永刚^{1,2} 林亮成^{1,2} 韩淞^{1,2}

[1. 国网思极检测技术(北京)有限公司; 2. 国网思极网安科技(北京)有限公司]

摘要: 【目的】随着“三法一条例”等法律法规及电力行业网络安全评价、技术监督等要求相继实施, 企业网络安全合规检查呈现“多线并行”态势, 包括等级保护测评、风险评估、数据安全评估、个人信息保护审计、安全评价、企业常态化督查等多种类型, 存在控制点交叉重叠、整改闭环割裂等问题。【方法】本文从标准化视角提出构建“多评合一”(Multiple Assessments Integration, MAI) 机制, 其依据等保2.0“一个中心、三重防护”以及风险管理方法论, 以“统一入口、分类实施、成果共享、闭环管理”为核心理念, 从而实现“一次检查、全面体检、统一整改、多方确认”的目标。【结果】研究设计了包括协同机制建设、标准体系映射、作业模式优化、数字化平台支撑这4个维度的实施框架, 着重处理好第三方机构测评协同与跨部门整改闭环管理难题, 建立起统一问题台账及整改跟踪体系。【结论】通过实践验证, 在保证安全标准不降低的情况下, 这一机制能把重复检查项减少50%以上, 且实现检查发现问题整改闭环率100%, 为企业网络安全治理体系现代化提供标准化解决方案。

关键词: 网络安全; 合规检查; 多评合一; 标准化; 治理体系; 风险评估; 等级保护

DOI编码: 10.3969/j.issn.2097-857X.2026.10.012

Redundancy Governance in Cybersecurity Compliance Inspections of Power Enterprises: Mechanism Innovation and Standardization Practice

LI Yonggang^{1,2} LIN Liangcheng^{1,2} HAN Song^{1,2}

(1. State Grid SLJI Testing Technology (Beijing) Co., Ltd.; 2. State Grid Cyber Security Technology (Beijing) Co., Ltd.)

Abstract: [Objective] With the implementation of relevant laws and regulations, the requirements for technical supervision and cyber security evaluation in the power industry have become more and more prominent. In the process of cyber security compliance inspection, enterprises are faced with the problem of “multiple lines in parallel”, which leads to the implementation of multiple assessments, but the results are not ideal. [Methods] This paper analyzes from the standardization level, and builds a “Multiple Evaluation Integration” mechanism, which is based on the “one center and three layers of protection” framework, and emphasizes the importance of risk management. It can achieve the goal of “one-time inspection, comprehensive inspection, and multi-party confirmation”. [Results] In this study, a four-dimensional framework is constructed, including digital platform support, operation mode optimization, standards system mapping and so on, to solve the problems of closed-

作者简介: 李永刚, 本科, 高级工程师, 研究方向为信息通信技术及电网网络安全。

林亮成, 硕士, 高级工程师, 研究方向为电网网络安全。

韩淞, 本科, 工程师, 研究方向为电网网络安全。

loop management and third-party assessment. [Conclusion] After practical verification, this mechanism can not only ensure the security standards, but also reduce the number of repeated items by more than 50%, and can also achieve 100% closed-loop management, which can provide reference for the construction of enterprise cyber security governance system.

Keywords: cybersecurity; compliance inspection; Multiple Assessments Integration (MAI); standardization; governance system; risk assessment; classified protection

0 引言

随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》(简称“三法一条例”)等法律法规,以及《电力监控系统安全防护规定》(发改委令第27号)^[1]的密集出台,电力企业网络安全合规要求日趋严格。当下电力企业同时要应对等级保护测评^[2]、信息安全风险评估^[3]、数据安全评估^[4]、个人信息保护审计^[5]、行业安全评价^[6]、电力企业常态化网络安全检查督查6类检查评价工作,从而形成了“多线并行”的监管格局。

通过对相关标准分析和实践发现,6类检查在技术方法、检查对象、数据采集等方面存在一定程度的同质性。技术层面的资产梳理、漏洞扫描、配置核查等基础内容重叠度达50%~60%,所以同一单位一年要接受多轮检查。并且由于监督检查评价等管理方不同,整改闭环被割裂,同类问题在不同检查中反复出现,缺乏统一跟踪和验收机制。另外,等保测评、风险评估通常由第三方机构实施,而数据安全评估、个人信息保护审计则涉及不同管理部门,这就造成监管视角碎片化、整改要求时效不一致等问题^[7]。

本文运用标准化系统工程方法,基于等保2.0“一个中心、三重防护”(一个中心:安全管理中心;三重防护:安全通信网络防护、安全区域边界防护、安全计算环境防护)技术框架^[8]以及风险管理理论,提出“多评合一”(MAI)机制。该机制秉持“统一入口、分类实施、成果共享、闭环管理”的核心理念,设计涵盖协同机制、标准体系、作

业模式、数字化平台的四维实施架构,并给出能力落地信息管理平台 and 检测工具整合的建设方案,从而为企业网络安全治理体系现代化提供标准化解决办法。

1 现状分析

当下电力企业所面临的网络安全检查评价工作主要涵盖6类(见表1)。以等保三级系统为例开展信息安全风险评估分析,并对71个控制点^[9]予以映射。在组织架构制度体系、应急响应等管理类要求方面,各类检查的重叠程度为60%至90%,而在资产梳理、漏洞扫描、配置核查等技术类基础内容方面,其重叠程度则为40%至65%。这些评估分析尽管依据不同的标准,但在技术手段、检查目标、数据收集等方面却具有相似性。

依据国家能源局针对电力企业安全生产的要求^[10]以及迎峰度夏的工作任务^[11],电力企业一般会 把评估、测评等放在春季与秋季,基层单位在这段时间集中开展多次检查工作。据统计,省级公司关键系统平均每年要接受各类检查3~5次,地市公司也达2~3次。

2 理论框架与制度基础

2.1 核心理念与基本原则

MAI机制打破了分散检查各自闭环的模式,通过统筹计划、分类实施、兼容差异、成果共享来实现数据互通,并构建起跨部门统一的闭环整改体系,打造“多评合一”机制,实现“一次检查、全面体检、统一整改、多方确认”的治理模式。

表1 网络安全检查评价工作类型一览

序号	检查类型	主要依据	实施频次及形式	责任主体	综合重合指数
1	网络安全风险评估	信息安全技术 信息安全风险评估方法 ^[3]	年度/专项	第三方机构	基准项
2	网络安全等级保护测评	信息安全技术 网络安全等级保护基本要求 ^[2]	二级以上定期	等保测评机构	70%
3	数据安全风险评估	数据安全技术 数据安全风险评估方法 ^[4]	年度/专项	第三方机构	60%
4	个人信息保护审计	信息安全技术 个人信息安全影响评估指南 ^[5]	定期/触发式	内部/第三方机构	62%
5	行业安全评价	电力监控系统网络安全评估指南 ^[6]	年度	安监部门	55%
6	常态化网络安全督查	电力企业网络安全管理制度	春秋检+专项	数字化部门	68%

(1) 统筹计划。构建一致的检查规划与进场体系, 统筹检查的时间, 防止重复进场。

(2) 分类实施。在统一框架下, 针对不同检查类型存在测评方法、深度要求等特殊要求的情形, 制定差异化检查策略。

(3) 成果共享。构建检查结果相互认可的机制, 使同一证据在不同检查类型中实现复用以防止重复采集。

(4) 闭环管理。编制统一的问题台账并进行整改跟踪, 并经多方确认, 以保证问题确实能够销号。

从具体实施的角度来看, 要遵循的原则包含:

(1) 减负增效原则。在不降低安全标准的前提下, 把迎检频次减少50%以上且消除重复整改。

(2) 同类合并原则。对于技术同源、内容相近及对象相同的情况, 将相关检查进行整合, 例如将等级保护测评^[12]和电力监控系统安全防护评估的同类检查项合并。

(3) 成果互认原则。建立检查结果的共享机制, 避免重复验证, 也符合了《电力行业网络安全等级保护管理办法》^[13]中“避免重复测评”的要求。

(4) 闭环统管原则。建立跨部门、跨检查类型的统一整改闭环管理机制, 确保问题发现、整改、验收、销号全流程统一;

(5) 工具赋能原则。以数字化工具支撑多维

度合规检查, 实现检查数据的标准化采集和自动化分析。

2.2 法律法规与标准体系分析

2.2.1 法律层面的兼容性

《中华人民共和国网络安全法》确立等级保护制度的基础性地位, 明确网络运营者义务; 《中华人民共和国数据安全法》要求数据处理活动基于等保履行安全义务; 《中华人民共和国个人信息保护法》强调个人信息处理合规审计与透明度; 《关键信息基础设施安全保护条例》在等保基础上对关键信息基础设施运营者实施重点防护。“三法一条例”的监管目标均为维护国家安全、公共利益与个人权益, 形成以等保为基础、专项要求作为补充的法律架构, 为“多评合一”提供顶层制度兼容性。

《电力行业网络安全等级保护管理办法》^[13]第十三条规定: 电力监控系统网络安全等级保护测评工作应当与电力监控系统安全防护评估、关键信息基础设施网络安全检测评估、商用密码应用安全性评估工作相衔接, 避免重复测评。

2.2.2 标准层面的映射关系

通过对比分析《信息安全技术 网络安全等级保护基本要求》^[2]《信息安全技术 信息安全风险评估方法》^[3]《工业控制系统安全检查指南》《电力监控系统网络安全评估指南》^[6]等标准, 建立起

“对照矩阵”基线。

(1) 共性项(占比约65%,可合并检查)。主要包括物理环境安全、网络安全、主机安全、应用安全、数据安全、安全管理等基础控制点。

(2) 特性项(需要专项检查,占比约25%)。比如电力行业的“横向隔离、纵向认证”、个人信息保护影响评估等特定要求。

(3) 差异项(约10%,需协调处理)。不同的标准在个别控制点要求上存在一些差异,需通过标准解释或技术规范予以协调处理。

上述3类划分为后续实施框架提供了分类整合依据,并以此建立差异化的作业模式。

2.3 标准化整合的技术可行性

各类检查评价均遵循风险管理过程方法以及PDCA(计划—执行—检查—改进)循环。信息安全管理体系^[14]的过程方法与持续改进机制,为MAI机制的流程整合提供了操作层面的方法论,并与等保2.0的技术架构形成了“技术—管理”二维管理矩阵。在此基础上,通过建立统一的检查底稿(Checklist)和证据库可以实现以下目标:

(1) 数据采集标准化。统一资产发现、漏洞扫描、配置核查的数据格式与接口。

(2) 评估流程规范化。统一评估准备、现场实施、风险分析、报告编制的流程。

(3) 结果输出自动化。基于统一检查底稿,自动生成符合不同监管要求的专项报告。

3 实施框架设计

3.1 机制层面:建立协同工作机制

3.1.1 组织架构设计

在电力企业数字化领导小组组织下,由网络安全归口管理部门牵头,安监、业务部门、基层生产单位参与,明确各部门/单位职责边界。牵头部门负责统一计划管理和资源协调,配合部门负责专业领域的技术把关。建立跨部门的协同机制,实现对检查结果的专业化分析、决策和实施。

3.1.2 制度文件体系

制定《网络安全多维度检查评价实施细则》,明确“多评合一”的适用范围、工作流程、质量控制和责任划分,并修订企业《网络安全评价管理办法》,确保检查管理满足各监管部门要求。

3.2 标准层面:构建统一技术规范

构建跨标准的要求映射图谱^[15]与问题编码体系,从而解决多类检查“技术同源、标准各异”的问题,达成检查要素标准化、问题描述统一化、整改要求规范化的目标,为“多评合一”提供可施行的技术依据与操作指引。

3.2.1 建立检查映射图谱

基于等保2.0“一个中心、三重防护”框架,构建6类检查的“要求对照矩阵”,并建立统一问题编码体系:

(1) 统一必查项。涵盖法律法规强制性要求和通用安全控制措施,建立统一问题描述模板;

(2) 专项检查项。包括针对不同检查类型的特殊要求,如等级保护的定级要求、风险评估的风险计算方法、个人信息保护的权益影响评估等;

(3) 深度检查项。建立高风险问题强制闭环标识。

3.2.2 统一检查标准与闭环管理规范

编制《网络安全综合检查评价技术指南》和《网络安全检查问题整改闭环管理规范》,需要明确的主要内容如下:

(1) 证据分级分类标准,实现基础证据、专项证据、深度证据的分类管理;

(2) 问题分级标准。统一高危、中危、低危分级标准,匹配不同整改时限(如高危30天、中危60天、低危90天);

(3) 整改闭环流程。建立“发现、录入、分派、整改、自检、复核、销号”的七步闭环管理流程;

(4) 跨部门协同规则。明确不同监管部门对同一问题的确认流程,避免重复验收。

3.3 实施层面:优化作业模式

通过对检查计划的编制和现场实施流程的统筹,建立联合进场、协同作业、分层实施的新模

式,实现从“分散作业”向“集约作战”转变,确保一次进场即可完成多维检查、统一归集问题并同步启动整改,最大化提升实施效率与闭环时效。

3.3.1 统一计划管理

制定年度的《网络安全综合检查计划》,统筹6类检查的时间。通过“联合检查团队”模式,组建包含各检查领域专家(包括第三方测评机构人员)的联合检查组,一次进场完成多项评价。

建立现场问题会商机制。针对检查过程中发现的问题,由联合检查组现场确认问题性质和整改要求,避免不同检查组对同一系统提出矛盾整改意见。

3.3.2 基于标准映射的分类实施策略

依据2.2.2节建立的共性项、特性项、差异项分类,实施差异化整合:

(1) 共性项合并实施。对于占比约65%的共性项,包括物理环境安全、网络安全、主机安全、应用安全、数据安全、安全管理等基础控制点,实施统一检查底稿、统一数据采集、统一问题整改,避免重复测评和重复整改。

(2) 特性项专项实施。对于占比约25%的特性项,如电力行业“横向隔离、纵向认证”等特定要求,在统一测评基础上由专业人员实施专项检查,既保持检查深度与专业度,又避免重复进场造成的业务干扰。

(3) 差异项协调实施。对于占比约10%的差异项,建立跨标准协调机制,通过技术会商明确统一整改标准,编制标准解释或技术规范予以协调,避免因标准差异导致整改要求冲突或重复整改。

3.3.3 分层分级实施策略

在电力企业的“总部—省—地”三级管理和“生产控制大区—管理信息大区”分区防护的模式下,采用差异化整合策略。

(1) 对于总部及承担总部核心枢纽职能的单位(调度、集控中心、数据中心等),实施深度整合,实现生产控制大区与管理信息大区全覆盖,重点核查单向隔离装置、纵向加密认证等跨区域边界,以及统一安全管理平台、调度数据网接入

安全,确保“横向到边、纵向到底”落到实处。

(2) 省级公司层面采取中度整合,严格区分两大安全区并分别组织检查。生产控制大区侧重控制区与非控制区边界防护及纵向加密装置合规性;管理信息大区聚焦网络准入、边界防火墙策略及安全管理中心建设,避免交叉重复进场。

(3) 地市公司沿等保测评主线开展轻度整合,嵌入电力监控系统安全防护评估要求,重点核查大区边界隔离措施与主机加固落实情况。

(4) 电力生产企业(火电、水电、新能源)则聚焦“边界、主机、终端”三大核心,检查工业防火墙、纵向加密装置、单向隔离装置的被突破风险,主机系统白名单或加固软件部署情况,跨区互联隐患,以及终端移动存储介质和外设接入管控情况,防止边界失守引发生产系统入侵。

3.3.4 统一成果管理与监管协同机制

基于统一检查底稿,建立统一问题台账与整改闭环数据库,实现“一次发现、统一编码、多方共享、闭环销号”。具体机制涵盖:

(1) 统一问题归集与标准化编码。把六类检查所发现的问题(涵盖第三方测评机构发现的等级保护、风险评估方面的问题)全部纳入闭环管理系统,并且依照等保2.0“一个中心、三重防护”的框架,以及边界防护、主机加固、纵向加密等电力行业技术监督控制点开展标准化的分类编码工作,保证同一技术问题在各类检查时都引用同一个编码,以防止出现重复记录和整改的情况。

(2) 整改闭环统一管控。构建涵盖“发现—分派—整改—复核—销号”全流程的跨监管部门跟踪机制,并且把专业报告(由第三方测评机构出具)纳入统一台账管理,从而消除传统模式里“第三方独立闭环、企业再整改”的双重负担。

(3) 监管成果按需适配。以统一基础数据与整改台账为基础,依需求生成契合不同监管口径的成果资料,如等级保护测评结论、风险评估简报、技术监督通报、数据安全评估摘要等,并且按照要求输出JSON-LD、XML、Markdown等格式的

数据。

(4) 成果跨层级共享与复用。构建涵盖“总部—省—地”三级的共享检查成果库,并把历史整改数据归入企业网络安全档案中。对于那些没有产生变更的系统或者设备而言,在后续展开检查的时候能够直接运用历史合规证明以规避重复进行现场核查的情况。

3.4 统一信息化管理平台

建设统一的信息化管理平台,实现网络安全数据统一的采集、分析、共享及问题的闭环管理,并配备终端检查工具实现现场作业标准化与数据全流程贯通,以数字化手段支撑“一次检查、闭环管理”的治理目标,全面提升网络安全合规检查效能。

3.4.1 统一信息管理平台(云端)

云端平台集成知识库、大数据分析引擎与业务应用,为MAI机制提供数字化落地支撑。主要包括以下4个模块:

(1) 检查知识库依托知识图谱技术,将等保2.0、电力行业技术监督标准及6类检查要求融为一体,建立控制点映射与统一问题编码体系,实现跨标准智能关联;

(2) 大数据分析引擎利用大模型对多源异构数据进行关联分析与风险画像,把隐蔽攻击面和系统性风险识别出来;

(3) 智能报告中心基于统一检查底稿,自动生成适配不同监管口径的整改通报与合规报告,同时支持差异比对、版本溯源和整改建议推荐;

(4) 闭环管理系统建立跨部门整改任务台账,跟踪整改进度,可按监管机构需求直接输出JSON-LD、XML、Markdown等格式数据。

3.4.2 智能检查工具箱(边端/移动端)

边端和移动端的智能检查工具箱^[16]基于大模型研发,通过MCP协议与Skill技术实现渗透测试、工控协议解析、流量深度分析等能力的统一调度和数据标准化封装。工具箱具备意图识别与任务规划能力,能自动完成渗透测试、漏洞扫描、配置基线核查、敏感信息检测及网络流量深度解

析等现场作业任务。

4 结语

针对电力企业网络安全合规检查“多线并行”导致的冗余问题,本文提出了“多评合一”(MAI)标准化解方案。以等保2.0“一个中心、三重防护”框架与风险管理理论为基础,秉持“统一入口、分类实施、成果共享、闭环管理”的核心理念,设计出包含协同机制、标准体系、作业模式、数字化平台在内的四维实施架构,并且建立跨标准的要求映射图谱以及统一问题编码体系,从而解决等级保护、风险评估、数据安全、个人信息保护、行业评价、常态化督查6类检查内容交叉重叠的问题,还提出“多方检查、统一整改”的闭环管理模式,将第三方测评纳入企业统一台账管理。在某电力企业《网络安全多维度检查评价实施细则》标准编制和试点验证后发现,这个机制在不降低安全标准的情况下能将重复检查项减少52%以上、整改闭环率达到100%,显著提升电力企业网络安全治理能力,形成统一的风险视图,为企业网络安全治理体系数智化提供可落地的标准化范式。

本研究主要以电力行业实践为基础,其在跨行业的适用性有待进一步验证。未来研究可以从3个维度深入:一是通过智能化升级,将大模型和MCP协议等技术相结合,构建起智能检查知识图谱及自动化风险分析系统,使检查作业的模式从“人工经验驱动”转变为“AI智能驱动”,提高复杂场景中的风险识别精准度。二是在生态化方面进行拓展,探寻跨企业、跨行业的检查结果相互认可机制及数据共享的标准,搭建网络安全合规检查的生态体系,促使监管视角从“碎片化”朝着“一体化”发展。三是开展国际化对接工作,探究ISO/IEC 27001《信息安全、网络安全和隐私保护—信息安全管理体系—要求》、NIST CSF《网络安全框架》等国际标准与国内等保2.0相融合的途径,给跨国企业制定出一体化的合规方案。

与此同时,《电力监控系统安全防护规定》(27号令)等新法规施行后,要不断优化标准映射图谱及闭环管理规范,保证MAI机制和监管要求能够动态适配。

参考文献

- [1] 国家发展改革委. 电力监控系统安全防护规定[Z]. 2024.
- [2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求[S].
- [3] GB/T 20984—2022 信息安全技术 信息安全风险评估方法[S].
- [4] GB/T 45577—2025 数据安全技术 数据安全风险评估方法[S].
- [5] GB/T 39335—2020信息安全技术 个人信息安全影响评估指南[S].
- [6] GB/T 38318—2019 电力监控系统网络安全评估指南[S].
- [7] 詹伟. 工程生态视野中的工业互联网[J]. 工程研究: 跨学科视野中的工程, 2025, 17(1): 55-64.
- [8] 马力, 陈广勇, 祝国邦. 网络安全等级保护2.0国家标准解读[J]. 保密科学技术, 2019(7): 14-19.
- [9] 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, 20(5): 1-10.
- [10] 国家发展和改革委员会. 电力安全生产监督管理办法[Z]. 2015.
- [11] 国家能源局综合司. 2025年电力安全监管重点任务[Z]. 2025.
- [12] DL/T 2613—2023 电力行业网络安全等级保护测评指南[S].
- [13] 国家能源局. 电力行业网络安全等级保护管理办法[Z]. 2022.
- [14] GB/T 22080—2025 网络安全技术 信息安全管理体系要求[S].
- [15] 朱若彬. 网络安全知识图谱构建关键技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2025.
- [16] 李永刚, 杨宇波, 潘善民. 基于大模型驱动的自动化漏洞挖掘系统研究[C]//中国计算机学会. 第40次全国计算机安全学术交流会论文集. 国网思极检测技术(北京)有限公司, 2025: 156-160.