固网终端管理风险的全流程闭环防控体系构建与实践

郭海歌
中国电信河南公司，河南 郑州 450000

[摘要]固网终端作为通信运营商重要的固定资产，涉及采购、入库、出库等多个环节，历来是廉洁风险高发领域。近年来，随着一些新型终端大规模部署，终端管理的复杂性进一步加剧，串码管理缺失、流程存在盲区、稽核能力不足等问题日益突出。针对上述问题，某公司 2025 年开展固网终端专项整治，构建了“事前预防、事中拦截、事后稽核”的全流程闭环防控体系。实施后，终端流失率下降 50%，追回损失超百万元。本文系统阐述了该体系的构建背景、核心理念、关键举措、实施成效和经验启示，为通信行业终端管理提供可借鉴的路径。

[关键词]固网终端；专项整治；全流程闭环；逐级校验；风险防控
DOI：10.64635/ja.2026.1116 中图分类号：F626 文献标识码：A

Construction and Practice of a Full-Process Closed-Loop Risk Prevention and Control System for Fixed-Network Terminal Management

Guo Haige
China Telecom Henan Company, Zhengzhou 450000, Henan, China

Abstract: As important fixed assets of telecommunications operators, fixed-network terminals involve multiple links, including procurement, warehousing, and outbound distribution, and have long been a high-risk area for integrity-related management issues. In recent years, with the large-scale deployment of certain new types of terminals, the complexity of terminal management has further increased, and problems such as the absence of serial number management, blind spots in operational processes, and insufficient auditing capability have become increasingly prominent. In response to these issues, a certain company launched a special rectification campaign for fixed-network terminals in 2025 and established a full-process closed-loop risk prevention and control system featuring “pre-event prevention, in-process interception, and post-event auditing.” After implementation, the terminal loss rate decreased by 50%, and recovered losses exceeded one million yuan. This paper systematically expounds the background of the system’s construction, its core concepts, key measures, implementation outcomes, and practical insights, with a view to providing a reference path for terminal management in the telecommunications industry.

Keywords: fixed-network terminals; special rectification; full-process closed loop; step-by-step verification; risk prevention and control

1 引言

1.1 研究背景

固网终端是通信运营商为用户提供宽带、语音、视频等业务所必需的物理设备，包括光猫、机顶盒、路由器、FTTR 主从设备等。随着光纤到户的普及和家庭数字化需求的提升，固网终端的部署规模持续扩大，其管理难度也随之增加。

从管理链条看，固网终端经历采购入库、仓储管理、出库配送、安装调试、用户使用、故障换机、拆机回收、报废处置等多个环节，每个环节都可能存在管理漏洞。从参与主体看，涉及采购部门、仓库管理人员、装维人员、营业人员、第三方物流等多类人员，管理半径大、监督难度高。从风险特征看，终端作为实物资产，具有价值高、易流转、难追溯的特点，一旦管理失控，极易产生“体外循环”和利益输送问题。

近年来，随着 FTTR（光纤到房间）、商业版 FTTR 等新型终端的大规模推广，终端管理的复杂性进一步加剧。这些新型终端不仅数量大、价值高，而且主配串码关

系复杂，对管理系统提出了更高要求。与此同时，廉洁风险防控的形势也日益严峻，终端领域成为腐败问题滋生的温床、问题的高发区。

1.2 主要问题

从某公司 2025 年初的摸底情况看，固网终端管理主要存在以下问题：

1.2.1 串码管理缺失，终端流向无法全程追溯

串码是终端的“身份证”，是追溯终端流向的唯一标识。然而，在实际管理中，部分新型终端的主配串码数据不完整，入库、出库、安装、回收各环节的串码信息未能有效关联，导致终端“从哪来、到哪去、谁在用、何时回收”无法全程追溯。一些终端在系统里“消失”后，实际上流向了非授权渠道或被违规占用。

1.2.2 流程存在盲区，关键节点管控缺失

在故障换机环节，传统流程缺乏对旧机回收的强制管控，存在“只出不进”或“以旧充新”的漏洞。部分装维人员在为用户更换故障终端后，未按规定回收旧机，导致旧机流失。在拆机回收环节，系统缺少对拆机用户与终端串码的强制关联，拆机后终端去向不明。这些流程盲区成为风险藏身的温床。

1.2.3 稽核能力不足，问题发现严重滞后

传统终端稽核以事后抽查为主，覆盖面和频次有限，大量异常交易无法被及时发现。即使发现问题，由于时间跨度长、证据链不完整，追责难度大。这种“事后诸葛亮”式的稽核模式，难以形成有效震慑。

1.2.4 数据壁垒明显，多系统无法贯通

营业前台系统、装维装机平台、仓库管理系统、稽核平台等各自为政，数据口径不一，无法实现全量比对。终端串码在不同系统之间存在“数据孤岛”，异常流转难以被系统自动识别和拦截。

1.3 研究意义

构建全流程闭环防控体系，不仅是防范廉洁风险、挽回企业损失的现实需要，更是推动治理模式从“事后被动应对”向“事前主动预防”转型的重要探索。本文以某公司 2025 年固网终端整治实践为案例，系统总结其经验做法，以期为通信行业终端管理提供可借鉴的路径。

2 全流程闭环防控体系的构建思路

2.1 核心理念：从“人防”到“技防”

传统终端管理依赖人工检查和事后追责，存在“看不到、管不住、查不准”的困境。人为因素多、标准不统一、执行不到位，是传统管理的三大痛点。本项目的核心理念是：将管理要求嵌入系统流程，用技术手段替代人盯人，实现全流程自动管控。

具体而言，就是将终端管理的各项规范转化为系统规则，在关键操作节点设置强制校验，违规操作无法继续；同时打通多源数据，实现全量比对，让异常无处遁形。这种“技防”模式，不受人员变动影响，不受地域差异干扰，具有稳定、高效、全覆盖的特点。

2.2 总体框架：三道防线、五个环节

构建“事前预防、事中拦截、事后稽核”三道防线，覆盖终端管理五个关键环节：

第一道防线：事前预防。新型终端全部纳入逐级校验体系；从源头确保串码准确、账实相符；对采购、入库环节进行系统管控

第二道防线：事中拦截。在故障换机环节设置旧机回收强制校验；在拆机环节设置串码录入强制要求；违规操作无法继续，系统自动拦截。

第三道防线：事后稽核。打通多源数据，实现全量比对；精准发现异常问题；派单追责，形成闭环

覆盖的五个关键环节：入库、出库、安装、故障换机、拆机回收。

2.3 设计原则

在体系设计过程中，始终坚持以下原则：

（1）全流程覆盖原则：从终端进入企业到退出企业的全过程，每一个环节都要有管控。

（2）系统嵌入原则：管控要求不靠人盯人，而是嵌入系统，让系统自动执行。

（3）数据贯通原则：打破系统壁垒，让数据在营业前台、装维装机、仓库管理等系统之间自由流动。

（4）闭环管理原则：发现问题不是终点，追责问责、完善机制才是闭环。

3 关键举措与创新实践

3.1 筑牢系统防线：逐级校验机制全覆盖

逐级校验是本项目最核心的创新举措。所谓“逐级校验”，是指终端从入库到出库再到安装使用的全过程中，在五个关键节点进行串码比对，确保终端流向全程可追溯。

第一级：入库校验。在终端入库环节，系统自动比对串码与采购订单的一致性。串码不在采购订单范围内的，无法入库。这一措施从源头上杜绝了“账外终端”的存在。

第二级：出库校验。在终端出库环节，系统自动比对串码与出库单的一致性。出库的终端必须有对应的出库单据，确保账实相符。

第三级：安装校验。在终端安装环节，系统自动比对串码与用户信息的关联。终端安装到哪个用户，串码就绑定到哪个用户，实现“终端到人”。

第四级：故障换机校验。在故障换机环节，系统强制要求先录入旧机串码、确认回收后，才能出库新机。旧机不回收，新机无法出库，杜绝了“只出不进”的漏洞。

第五级：拆机校验。在用户拆机环节，系统强制要求录入拆机用户的终端串码，确保拆机终端可追溯、可回收。

3.2 补齐流程短板：关键节点系统嵌入

针对流程盲区，开展系统性补漏：

3.2.1 故障换机流程优化

在装维装机平台上线“故障换机审批与串码校验流程”。装维人员为用户更换故障终端时，必须先扫描旧机串码，系统验证旧机状态和用户信息，确认无误后方可出库新机。旧机回收后，系统自动生成回收记录，进入待处置状态。这一流程从根本上解决了故障换机环节的漏洞。

3.2.2 拆机流程优化

在营业前台系统增加“拆机用户串码录入功能”。用户办理拆机时，营业人员必须录入拆机终端的串码，系统自动校验该串码是否与用户绑定的终端一致。不一致的，系统提示异常，需核实原因后方可继续。这一措施确保拆机终端与用户信息一一对应，便于后续回收稽核。

3.2.3 回收流程固化

协同相关部门，梳理并固化设备回收及串码校验全流程，明确各环节责任主体、操作规范和时间节点，形成标准化作业指导书。从装维人员回收终端，到仓库入库登记，再到系统状态更新，每一个步骤都有明确的操作要求和时间限制。

3.3 打通数据链路：多源数据贯通稽核

数据贯通是本次整治的又一关键举措。协同相关部门，开展以下工作：

（1）统一数据口径：对营业前台、装维装机、仓库管理等系统的数据口径进行统一，明确异常数据的判断标准。

（2）增加稽核点：增加全流程稽核点增加 10 个，覆盖终端管理的更多细节环节。新增的稽核点包括：采购订单与入库比对、出库与安装比对、安装与激活比对、故障换机旧机回收状态、拆机终端回收状态等。

（3）贯通监管平台：实现与监管平台的数据贯通，将稽核结果自动推送至监管平台，形成从数据发现到派单追责的闭环。

3.4 深化专项治理：协同监督追责挽损

系统建设和技术手段是基础，但人的因素同样重要。本次整治坚持技术手段与组织手段并重，协同纪委推动问题整改问责。

3.4.1 异常数据下发

全年下发异常数据数万条，涵盖终端安装异常、故障换机异常、拆机回收异常等多个类型。每一批次异常数据都附有明确的核查要求和反馈时限。

3.4.2 培训赋能支撑

针对地市核查能力不足的问题，组织多场专题培训，讲解异常数据的判断标准、核查方法和整改要求。通过培训，地市人员的核查能力和专业水平得到显著提升。

3.4.3 问题核查处置

对发现的异常数据，坚持“发现一个、处置一个”。核查过程中，逐条核实问题原因，区分系统问题、流程问题、人为问题等不同情形。对系统问题，及时优化完善；对流程问题，优化调整；对人为问题，严肃追责问责。

3.4.4 追责问责与挽损

追回流失终端，挽回损失超百万元。对违规行为形成有力震慑，让制度“长牙”、纪律“带电”。

4 实施成效

4.1 风险指标显著改善

经过一年的专项整治，固网终端领域的风险指标得到显著改善：

（1）异常激活率：下降 50%。异常激活是指终端在非用户地址被激活，是终端外流的重要信号。这一指标的显著下降，说明终端违规外流风险得到有效控制。

（2）异常数据发现：全年下发异常数据数万条，精准发现典型问题数十例。这些问题中，既有系统漏洞导致的误判，也有人员违规操作导致的异常，为后续完善机制提供了宝贵依据。

（3）追责问责：追责问责百余人次，涉及装维人员、营业人员、仓库管理人员等多个岗位。严肃追责形成了有力震慑，违规行为明显减少。

（4）追损挽损：追回流失终端，挽回损失超百万元，有效维护了企业资产安全。

4.2 管理体系系统升级

（1）稽核能力：稽核点覆盖更全面，管控更精细。从原来的单一环节稽核，扩展到全流程、多节点的立体稽核。

（2）逐级校验：全量终端设备强校验，逐级校验机

制成为终端管理的“防火墙”。

（3）数据贯通：营业前台、装维装机、仓库管理、稽核平台等多系统数据打通，形成“发现—派单—追责”闭环。数据孤岛被打破，异常无处遁形。

4.3 治理模式成功转型

通过系统嵌入和数据贯通，治理模式实现根本性转变：

（1）从事后到事前：过去是问题发生了再去查，现在是问题发生前就拦截。逐级校验机制在终端流转的关键节点设置强制校验，违规操作无法继续。

（2）从人防到技防：过去依赖人工检查和自觉性，现在依靠系统规则和自动化比对。技术手段替代人盯人，管理更稳定、更高效。

（3）从抽查到全量：过去是抽样稽核，覆盖面有限；现在是全量数据比对，不放过任何一个异常。

（4）从单兵作战到协同作战：过去各部门各自为战，现在业务、技术、纪委等多方协同，形成监督合力。

5 经验与启示

5.1 技术赋能是根本

将管理要求嵌入系统流程，用技术手段堵住漏洞，是解决终端管理顽疾的根本出路。单纯依靠人工检查和事后追责，难以实现长效治理。技术赋能的核心在于：把规则写进代码，让系统自动执行；把数据打通，让异常自动浮现。

5.2 数据贯通是关键

打通营业前台、装维装机、仓库管理、稽核平台等多源数据，实现全量比对，才能让异常无处遁形。数据孤岛是风险藏身的温床，数据贯通是风险防控的利器。在数据贯通的基础上，建立异常数据识别模型，可以实现风险的自动预警。

5.3 协同监督是保障

业务部门与纪委、审计等部门协同联动，形成监督合力，才能实现有效追责和长效治理。单打独斗难以形成闭环，协同作战方能标本兼治。业务部门负责系统建设和流程优化，纪委负责监督问责，审计负责独立核查，三方协同，形成完整闭环。

5.4 持续优化是常态

风险防控不是一劳永逸的，需要根据新情况、新问题持续迭代完善。随着新型终端不断涌现，管理手段也需要与时俱进。本次整治中发现的问题，很多都是在日常管理中被忽视的“细节”，正是这些“细节”构成了风险的“针眼”。只有持续优化、持续完善，才能做到“堵住针尖大的窟窿，漏过斗大的风”。

5.5 文化建设是根本

制度建设是“硬约束”，文化建设是“软环境”。在推进系统建设的同时，也要加强廉洁文化建设，让“不想腐”成为员工的自觉。通过案例警示教育、岗位风险提示等方式，增强员工的合规意识和廉洁意识，从源头上减少违规行为的发生。

6 结语

固网终端整治是一项系统工程，需要技术、管理、监督多管齐下。某公司 2025 年的实践表明，构建全流程闭环防控体系，能够有效防范风险、挽回损失、提升管理效能。这一经验可为行业提供有益借鉴。

未来，应进一步探索运用人工智能、大数据分析等新技术，推动终端管理向智能化、精准化方向升级。例如，利用机器学习算法识别异常终端流转模式，利用知识图谱构建终端流向网络，利用区块链技术确保终端流转不可篡改。这些新技术的应用，将进一步提升终端管理的科技含量和风险防控能力。

同时，要持续完善制度机制，强化协同监督，深化廉洁文化建设，为企业高质量发展保驾护航。终端管理的本质是资产管理，资产管理的核心是风险防控，风险防控的落脚点是制度建设和技术赋能。只有多管齐下、久久为功，才能真正实现终端管理的长治久安。

[参考文献]

[1]王晓明.通信企业终端资产管理风险防控研究[J].通信企业管理,2023(5):42-45.

[2]李建国,张丽华.基于全流程管控的廉洁风险防控体系构建[J].企业管理,2024(2):67-70.

[3]赵志强.大数据在通信运营企业内部控制中的应用[J].信息通信技术与政策,2024(8):51-55.

[4]刘敏.运营商终端串码管理优化路径探讨[J].电信技术,2023(11):38-41.

[5]陈志远.通信企业资产全生命周期管理研究[J].通信企业管理,2024(3):29-33.

[6]吴晓明.数字化转型背景下企业内部控制优化路径[J].会计之友,2024(7):82-86.

作者简介：郭海歌（1987.04—），女，汉族，河南洛阳人，硕士研究生，网络运营与终端管理。