ICS 35.240.99
CCS L73

团　　体　　标　　准

T/ISC 0121—2026

智能化穿透式监管技术能力要求

Technical Capability Requirements for Intelligent Penetrative Supervision

（发布稿）

2026-07-20 发布　　2026-08-20 实施

中 国 互 联 网 协 会　　发布

目　　次

前　言

本文件按照GB/T 1.1—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。

本文件为首次发布。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、中国联合网络通信集团有限公司、天翼支付科技有限公司、中电信数智科技有限公司、联通数字科技有限公司、北京凡得科技有限公司、上海软中信息技术有限公司、南网数字运营软件科技（广东）有限公司、南京市河西新城区国有资产经营控股（集团）有限责任公司。

本文件主要起草人：徐恩庆、海兴胜、何川、杨昊林、朱庭俊、海广跃、陶继业、宋俊典、黄德山、侯金鑫、陈柳英、李广义、蔡浩淼、徐文杰、张洋、尚啸、边鹏旭、王忠军、丁剑波、杨玉春、吕道峰、龚梅、石卉。

引　言

加强国有企业监管、保障国有资产安全增值，是推进国家治理体系和治理能力现代化的重要举措。近年来，穿透式监管理念逐步融入国资企业监管实践，成为突破监管层级、打通监管壁垒、实现全方位监管的核心导向；与此同时，人工智能、大数据等新一代数智技术加速迭代，与国有资产监管工作深度融合，不仅为穿透式监管的高效落地提供了坚实技术支撑，更推动监管模式从传统人工监管向数字化、智能化转型，亟需通过统一标准引领监管实践规范化发展。

为顺应国有资产监管智能化、数字化发展趋势，破解当前监管技术应用缺乏统一规范的问题，特制定本标准。本标准明确了智能化穿透式监管技术能力的核心导向与基本规范，为各类相关实践提供权威、可操作的指引，其实施兼具重要现实意义与长远价值。

本标准的实施，能够有效规范智能化技术在国有企业穿透式监管中的应用，统一技术应用基准与尺度，提升监管技术部署的统一性、协同性与合规性；能够显著强化国有资产监管的穿透能力与风险防控水平，降低监管成本、提升监管效能，推动监管模式实现根本性转型；更能进一步完善国有资产监管标准体系，为国有企业改革深化、高质量发展提供有力支撑，助力服务高水平社会主义市场经济体制建设，为推进国家治理体系和治理能力现代化奠定坚实基础。

智能化穿透式监管技术能力要求

1 范围

本标准规定了企业监管平台或企业业务应用为支撑国资国企实施智能化穿透式监管，所应具备的核心技术能力要求。

（1）产品设计与开发：为企业数智供应商提供产品规划、设计与开发的功能性技术规范；

（2）产品选型与评估：为企业在建设或采购具备智能化穿透式监管技术能力的产品时，提供技术选型与能力评估的依据；

（3）符合性测试与认证：为第三方测试机构对相关企业业务应用进行智能化穿透式监管能力的符合性评估提供标准化的测试准则。

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而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。

GB/T 36073—2018 数据管理能力成熟度模型

GB/T 44109—2024 信息技术 大数据 数据治理实施指南

GB/T 37721—2019 信息技术 大数据分析系统功能要求

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

下列术语和定义适用于本文件。

3.1 智能化穿透式监管 intelligent penetrative supervision

以穿透式监管为主线，以智能化转型为抓手，运用大数据、人工智能等现代信息技术，打破组织层级和系统壁垒，实现对国有企业“人、财、物、权、责”等关键管理要素数据的采集、分析、可视化与协同处置，形成覆盖“组织全级次、数据全链路、管理全要素、风险全透视”的监管新范式。

3.2 监管数据视图 supervision data view

基于统一数据标准和模型整合后形成的、用于支撑穿透式监管分析的数据集合，通常来源于对企业多个业务应用系统的数据集成与治理。

3.3 数据血缘 data lineage

描述数据从源系统到最终使用过程中的流转路径、变换逻辑与依赖关系，是支持数据可信溯源与质量评估的基础。

3.4 风险画像 risk profile

基于多维度数据对监管对象（如企业、项目、人员）进行标签化建模，形成其风险特征的综合视图。

4 符号和缩略语

下列符号和缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

API：应用程序编程接口 （Application Programming Interface）

ERP：企业资源计划 （Enterprise Resource Planning）

KPI：关键绩效指标 （Key Performance Indicator）

NLP：自然语言处理 （Natural Language Processing）

5 概述

智能化穿透式监管能力框架应涵盖数据底座、智能分析、穿透可视化、协同处置及平台架构与安全五大核心能力域（见图1），形成“数据驱动、智能预警、闭环管理、可视可控、安全合规”的一体化监管体系。

穿透可视化域：实现数据交互展示与关系图谱

协同处置域：支撑流程化闭环与跨层级协作

智能预警域：提供风险识别、模型管理与分析工具

数据底座域：负责多源数据集成、治理与溯源

开放与安全域：保障监管开放、合规与可扩展

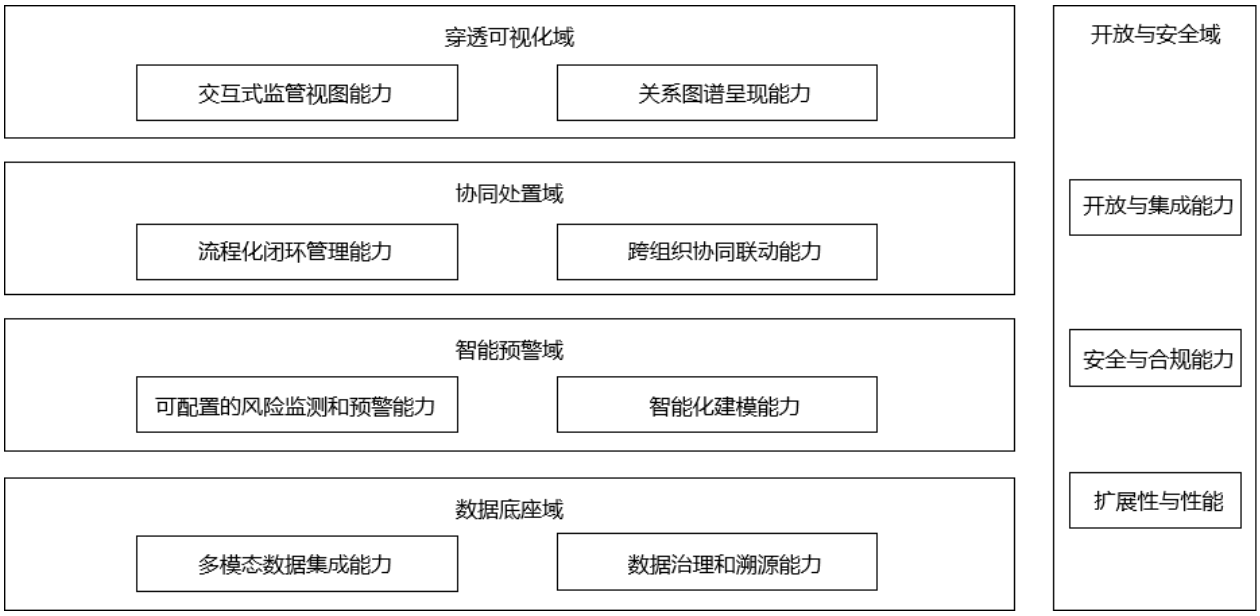

图 1 智能化穿透式监管能力框架

6 能力要求

6.1 数据底座域

6.1.1 多模态数据集成能力

平台应提供多种数据集成方案，以适配不同业务系统的技术特点和数据时效性要求：

a） 内部数据：应支持通过API接口、数据库日志捕获、文件传输等多种方式，从企业核心业务系统（如ERP、CRM、HRM）中采集财务、供应链、人事、资产等关键监管数据。

b） 外部数据：应提供标准接口，支持接入至少两种主流的外部数据源（如工商信息、司法信息），并具备扩展接入其他数据源的能力。

c） 采集频率：应支持实时、准实时（延迟不超过1小时）和批量（T+1）等多种数据采集策略，并允许按数据源和数据类型进行配置。

d） 数据格式兼容性：应支持多源异构多模态数据的接入与处理。

6.1.2 数据治理和溯源能力

a） 数据全生命周期管理：平台应支持数据采集、存储、加工、使用、归档、销毁各环节。

b） 主数据管理：平台应提供工具，支持对核心主数据（如组织、人员、会计科目、客户、供应商）进行统一管理和分发。

c） 数据血缘与穿透：平台应记录关键监管指标的数据血缘关系。对于从业务系统采集的核心财务和业务明细数据，支持从监管平台的汇总指标向下钻取至少三个层级，并最终能关联到至少一类原始业务凭证（如会计凭证号、采购订单号）的摘要信息，具体层级可根据实际业务需要配置。

d） 数据质量监控：应提供数据质量规则引擎，支持对完整性、一致性、准确性、时效性等维度进行自动校验与告警。

e） 数据质量责任追溯与闭环整改：宜支持数据质量问题的自动定位、责任主体识别、整改工单派发、整改效果验证的全流程闭环管理。

f） 元数据管理：应建立企业级元数据仓库，支持业务术语表、数据字典与数据血缘可视化查询。

g） 跨境数据追溯：宜支持跨境数据血缘追溯，满足境外业务监管需求。

6.2 智能预警域

6.2.1 可配置的风险监测与预警能力

平台应提供一个可扩展、可配置的风险规则引擎，并预置或支持配置对以下重大风险的监测与预警：

a） 应提供风险指标库，对“过度负债”、“财务金融风险”、“违规挂靠”等至少五类风险提供示例性的、可量化的监测指标（如“资产负债率”、“应收账款周转率”、“固定资产闲置率”）。

b） 规则引擎应支持基于阈值、趋势、比例、SQL表达式等多种条件组合配置预警规则。

c） 对于“靠企吃企”、“虚假贸易”等复杂风险，平台应提供利用知识图谱、关联分析等技术的分析工具和模型框架，辅助用户发现疑点。

d） 宜支持“三重一大”（重大事项决策、重要干部任免、重要项目安排、大额资金使用）决策全流程数据采集、合规校验与风险预警。

e） 预警通知：应支持通过短信、邮件、系统消息、API推送等多种方式触发预警，并支持分级预警机制。

6.2.2 智能化建模能力

a)场景化风险建模：平台应能基于数据构建并运行风险评估模型，为监管对象生成多维标签与量化风险画像，并以“红黄绿”码等形式动态展示风险状况与趋势。

b)模型管理：平台应具备对AI模型进行统一开发、部署、版本控制及持续监控（如准确率、召回率漂移预警）的能力。

c)分析工具集成：平台应集成或提供标准接口，支持运用机器学习、自然语言处理（NLP）等技术，对结构化与非结构化数据（如文本）进行特征提取、情感分析等建模分析。

d)自助分析：平台应提供低代码（如拖拽式）或自然语言交互界面，支持业务人员自主进行数据探索、特征工程与简易模型构建。

e）流程穿透与时序动态诊断：平台宜支持基于时间戳还原端到端业务流转轨迹，实现对合同流、资金流、货物流在时间与节点上实质性转移的精准校验。

f）风险传导与连锁反应建模：平台宜支持构建国资企业风险传导网络模型识别债务、担保、供应链、股权关联等维度的风险传导路径，量化风险传导强度与影响范围，实现对系统性风险的提前预判与分级预警。

g）模型可解释：宜支持对风险预警等模型提供可解释性输出（如触发预警的核心数据依据、权重占比、推理逻辑等），并完整记录模型的训练数据、参数配置、版本迭代、决策过程等全链路信息，宜支持对模型决策结果的回溯审计。

6.3 协同处置域

6.3.1 流程化闭环管理能力

a） 平台应提供工作流引擎，支持工单根据预设工作流及规则进行分派，并支持处理、转发、反馈、延期申请、销号等全流程管理。

b） 平台应提供处置进度看板，对超期任务进行自动提醒。

c） 知识库集成：应支持将典型处置案例沉淀为知识条目，供后续参考复用。

6.3.2 跨组织协同联动能力

a）平台应支持在国有资产监督管理机构、国有资本投资/运营公司、企业之间，实现监管指令的线上精准下达、任务接收、处置情况反馈的全流程线上化管理，确保指令流转可跟踪、处置结果可追溯。

b）宜支持任务分发、协办、会签、抄送等协同模式。

c）宜提供消息中心，支持系统内消息与外部通讯工具集成。

d）宜支持跨组织协同，支持与外部监管机构、合作伙伴的高效联动；

e）平台应提供标准化数据交换接口（如基于API、安全文件传输），支持按需、定时或触发式向授权的外部系统推送监管数据视图、风险预警或画像信息。

6.4 穿透可视化域

6.4.1 交互式监管视图能力

a） 平台应提供可配置的领导驾驶舱，支持多种图表组件。

b） 所有核心KPI指标（应在产品文档中明确定义何为“核心KPI”）必须支持逐层钻取（Drill-down）和维度切换（如按时间、按组织）。

c） 视图应支持用户交互，如数据筛选、图表联动、下钻上卷等。

d） 移动端适配：应提供响应式设计或专用移动端界面，支持在平板、手机等设备上访问关键监管视图。

e） 穿透分级管理：宜支持基于角色的穿透权限精细化管控，按监管层级、岗位职责、业务范围设置不同的数据穿透深度；宜支持对涉密项目、高管薪酬等敏感数据设置单独的穿透审批流程与操作留痕。

6.4.2 关系图谱呈现能力

a）平台应能通过可视化图谱，清晰展示企业内部组织架构、部门层级关系、产业上下游的企业拓扑、供应链关系等信息。

b）平台应能通过可视化图谱，清晰展示复杂的股权结构、关联方关系、担保链条、资金流向、人员兼职网络等，辅助识别潜在的风险传导路径和隐蔽关联。

c）图谱应支持主体穿透、动态布局、路径高亮、社区发现、影响力分析等功能。

d）应提供图谱数据导出与接口调用能力，支持第三方系统集成。

6.5 开放与安全域

6.5.1 开放与集成能力

平台应提供完整、清晰的接口文档，支持其他系统对监管数据、预警信息、风险画像等的查询与调用。应提供API文档和沙箱环境供第三方测试。

6.5.2 安全与合规能力

平台应具备完善的安全保障机制：

a） 应实现基于角色的权限控制，遵循最小授权原则，并对敏感数据实施传输、存储和展示时的脱敏或加密。

b）应提供不可篡改的系统操作与数据访问审计日志，确保所有监管行为可追溯。

c）应具备数据备份与灾难恢复机制，保障系统高可用性与业务连续性；

d）应支持建立与外部组织的安全责任协议与审计协同机制，确保数据在流转全链路的安全可追溯。

e）企业开展数据跨境传输活动，应遵循“分类管理、安全评估、合法有序、风险可控”的原则。

f）基于隐私计算、区块链技术，构建数据安全合规有序要素流通机制。

g）兼容适配：平台应支持基于安全可信的基础软硬件环境运行。

6.5.3 可扩展性与性能

平台应支持在不同部署规模下满足相应性能要求：

a） 性能体现，应支持穿透的企业最大层级数、并发用户数、单条预警响应时间、千万级数据查询响应时间、日数据处理吞吐量等满足相关要求。

b） 集群部署：应支持横向扩展的集群部署能力。