电信企业数据防泄露能力成熟度评估研究

王雪琼[1]，刘坚桥[2]，周旭华[1]
（1. 中国电信股份有限公司研究院，上海 200123；
2. 中国电信股份有限公司江西分公司，江西 南昌 330029）

摘　要：数据资源作为国家战略性资源，其重要性日益凸显。随着数字化转型的深入推进，数据泄露风险也日趋严峻。这一问题不仅直接威胁个人隐私，更可能因重要数据与国家核心数据的泄露，对国家安全产生深层次危害。现有研究多聚焦于数据泄露防范，而对其能力评估的研究则相对匮乏。为此，基于中国电信在数据防泄露领域的实践经验，构建了一个涵盖管理体系、技术支撑、运营保障3大能力领域，以及数据全生命周期、业务应用、数据流动和通用4大过程领域的数据防泄露能力成熟度模型。以中国电信某子公司数据流动过程维度数据防泄露实践为例，通过实证分析与评估，验证了该模型在实践应用中的科学性与可行性。

关键词：数据防泄露；数据保护；成熟度模型；能力评估；电信企业
中图分类号：TP309
文献标志码：A
doi: 10.11959/j.issn.1000−0801.DXKX250480

Research on maturity assessment of data leakage prevention capability for telecommunications enterprises

Wang Xueqiong[1], Liu Jianqiao[2], Zhou Xuhua[1]
1. Research Institute of China Telecom Co., Ltd., Shanghai 200123, China
2. Jiangxi Branch of China Telecom Co., Ltd., Nanchang 330029, China

Abstract: Data resources are recognized as a national strategic asset, whose significance has become increasingly prominent. With the accelerated advancement of digital transformation, data leakage risks have also grown more severe. This issue not only poses direct threats to personal privacy but may also cause deep-seated harm to national security due to the exposure of critical and national core data. Existing research primarily focuses on data leakage prevention measures, while studies on capability assessment in this domain remain relatively scarce. To address this gap, based on China Telecom's practical experience in data leakage, a data leakage protection capability maturity model was constructed. The model covered three capability domains: management system, technical support, and operational guarantee, as well as four process domains: the entire data lifecycle, business application, data flow, and general practices. Through empirical analysis and evaluation conducted on data leakage protection practices within the data flow process at a subsidiary of China Telecom, the model's scientific validity and feasibility are demonstrated in practical implementation.

Key words: data leakage prevention, data protection, maturity model, capability assessment, telecommunications enterprises

收稿日期：2025−07−29；修回日期：2026−01−13

0 引言

在数字经济时代，数据已成为核心生产要素，数据安全问题上升至国家安全的战略层面。在全球数据流动日益频繁的背景下，数据防泄露能力不仅是组织数据安全防护体系的重要组成部分，更成为决定其生存能力与可持续发展的关键因素。现有研究大都围绕数据保护的技术框架与实施措施展开，覆盖数据传输、存储、使用、共享及公开等数据生命周期环节。相关研究进展如下：文献[1]研究了数据准备、使用、存储与销毁阶段的安全技术及其应用。文献[2]提出了视频监控数据跨域传输控制系统，从硬件和软件两个角度阐述了视频数据跨域安全传输的方法。文献[3]结合用户隐私数据特性，采用同态加密与深度学习融合技术实现隐私数据点对点加密传输，保障数据传输安全。文献[4]研究了主流数据库系统在访问控制、数据存储、数据脱敏、差分隐私等方面的技术实现原理。文献[5]探讨了云环境中多模态数据的安全存储技术，构建了包含服务器端、客户端、云存储服务插件以及元数据存储插件的云存储架构。文献[6]针对5G工业互联网数据分析中的隐私安全问题，提出了一种融合隐私计算与逻辑回归技术的轻量级方案。文献[7]提出了一种云边协同的数据安全共享方案，实现了数据细粒度访问控制和隐私保护。文献[8]研究了基于联盟区块链和密文策略属性加密的数据共享系统，实现细粒度访问控制并保障用户数据隐私。文献[9]深入分析了当前数据交换模式在安全传输保障方面存在的不足，提出了针对系统进程与数据资源的加固防护体系构建方案。文献[10]探讨了在公共数据开放的背景下企业面临的数据安全风险。文献[11]强调政府机关在信息公开过程中应加强敏感信息的保护，并提升公众防范信息泄露的能力。文献[12]提出了一种基于个性化隐私预算分配的差分隐私混合属性数据发布方法，以防止隐私数据泄露。

当前研究成果主要集中于数据保护领域，通过管理策略与技术方法防范数据泄露风险。然而，针对数据防泄露措施有效性评估的系统性研究仍存在不足，现有相关成果大多集中于其他领域。文献[13]构建了一套科研大数据治理成熟度指标体系，为相关评估提供理论与实践参考，以助力治理水平提升。文献[14]通过分析成熟度模型技术现状及资产管理数字化转型框架要素，构建了适用于资产管理数字化的成熟度模型。文献[15]基于成熟度模型，从政府、平台设施、用户三个维度构建了政府数据开放平台成熟度评估指标体系，细化评估标准，为优化数据开放平台提供参考。文献[16]基于管理信息系统生命周期，提取五个评估维度及其核心指标，构建了从无序级到优化级的五级成熟度模型。此外，文献[17]作为跨行业通用的国家标准，以数据安全体系化能力建设为目标，构建了5级评估框架。不过，该标准并非专门针对数据泄露风险防控设计，且缺乏行业适配机制，导致电信企业在落地共性要求时，普遍面临将通用框架转化为具体业务场景实施路径的困境。

综上所述，本文通过深入研究数据保护和成熟度模型相关理论，紧密结合中国电信数据防泄露工作实践，构建了一套适用于企业落地实施的数据防泄露能力成熟度评估标准。与现有研究相比，本文主要有以下两点贡献。

（1）围绕个人信息、企业商业秘密、重要数据及核心数据等敏感数据的防泄露问题，构建了一个包含“数据防泄露能力维度、过程维度与能力等级维度”的数据防泄露能力成熟度评估模型。现有研究大多聚焦于数据处理过程中的具体保护机制，尚缺乏面向数据防泄露能力的系统性评估框架。企业在实践中虽叠加部署多种管理与技术防护措施，但对自身防护体系中的短板与能力水平缺乏科学认知。本文提出的评估模型通过

多维度分析，为企业数据防泄露体系的优化升级提供科学性和可操作性的参考依据。

（2）立足中国电信数据防泄露能力建设实践，深度剖析企业数据防泄露管理全流程。以中国电信数据防泄露能力体系框架为基础，在数据防泄露过程维度中，系统梳理并提炼出涵盖数据分类分级、访问控制、传输加密、风险监测、数据流动等在内的35项关键过程，精准覆盖电信企业数据防泄露工作场景。同时，从管理体系、技术支撑、运营保障3大能力维度出发，结合企业管理要求、技术支撑水平、业务运营模式等实际情况，制定了不同能力等级下的数据防泄露评估标准。通过多维度、多视角的综合评估，全面、客观地反映企业数据防泄露能力的实际水平，为企业数据防泄露体系的优化升级提供可落地、可操作的科学依据。

1　电信企业数据防泄露能力成熟度模型

当前，产业数字化与数字产业化呈现出蓬勃发展的态势。在数字经济时代，数据已经成为基础性资源、重要生产力和关键生产要素，如何在保障安全的前提下推动数据要素有序流动与价值释放已经成为新时代的重要命题。电信企业作为综合信息服务运营商，掌握着关键基础通信设施数据及大量用户的个人信息，这些高价值数据资源极具吸引力，备受攻击者觊觎，致使行业内数据泄露事件频繁发生。因此，保障数据的合规使用，有效防范数据泄露事件，成为电信企业数字化转型过程中关注的重点。为应对数据泄露风险，电信企业从管理、技术、运营等多个维度着手，构建数据防泄露能力，并设计了数据防泄露能力成熟度评估方法，用于检验企业数据防泄露工作的落实情况，评估能力现状，为后续工作的持续优化提供依据。

1.1　能力成熟度评估的必要性

《中华人民共和国数据安全法》明确要求企业履行数据安全责任，防范数据泄露风险。电信企业因其行业特性，需主动构建完善的数据防泄露能力体系，从源头遏制数据泄露事件的发生。发生数据泄露事件时，第一时间追究相关部门及人员的数据安全责任，通过查漏补缺优化数据防泄露能力体系，形成“事件处置—能力补强”的闭环管理机制。

数据防泄露能力成熟度评估与数据安全责任、能力体系建设以及数据泄露事件之间存在着紧密且深层次的关联。成熟度评估与数据安全责任、能力体系、数据泄露事件间的关系如图1所示。成熟度评估，一方面可引导企业建立科学规范的数据防泄露能力体系，通过标准化建设提升风险防控效能；另一方面能强化企业内部各部门数据安全责任的刚性落实，通过责任传导机制减少人为疏漏导致的安全隐患。同时，数据泄露事件的处置经验，可反向推动成熟度评估标准的迭代升级，形成“实践反馈—标准优化”的动态进化机制，最终实现数据安全防护能力的持续提升。

数据防泄露能力成熟度评估将复杂的安全问题转化为可管理的阶段目标，通过动态反馈机制推动企业系统性提升数据防泄露能力，实现从“被动响应”到“主动作为”的转变，进而达到构建内生的数据防泄露能力体系的目的。

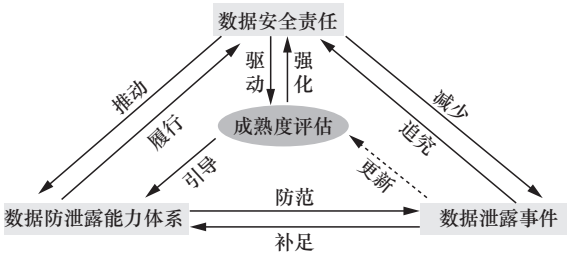

图1　成熟度评估与数据安全责任、能力体系、数据泄露事件间的关系

1.2　数据防泄露能力成熟度模型框架

本文构建的电信企业数据防泄露能力成熟度模型框架如图2所示，从数据防泄露过程、数据

防泄露能力两个维度出发，将能力成熟度划分为5个等级，从低到高依次为基础级、可管理级、成长级、先进级和卓越级，每个等级的内涵如下。

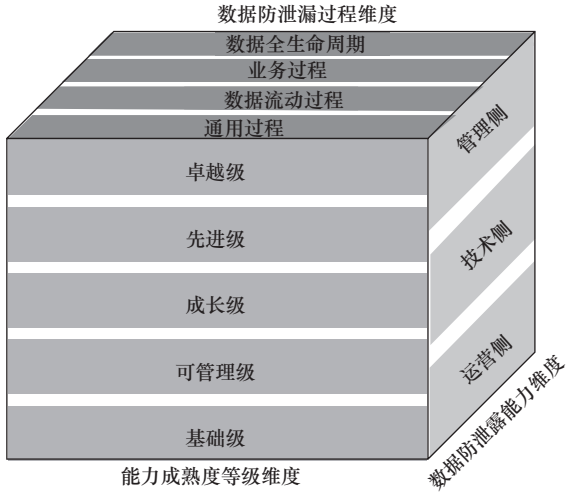

图2　电信企业数据防泄露能力成熟度评估模型框架

（1）基础级：企业的数据防泄露能力处于起步阶段，缺乏规划；

（2）可管理级：企业具备基本的数据防泄露能力，但未形成体系化；

（3）成长级：企业实现了数据防泄露工作的系统化和规范化；

（4）先进级：企业实现了数据防泄露能力的量化度量和优化；

（5）卓越级：企业数据防泄露能力达到行业领先水平。

电信企业可参考本文构建的数据防泄露能力成熟度模型评估自身数据防泄露能力目前所处的阶段，明确后续需要重点提升或改进的方向。

1.3　数据防泄露能力维度

大部分数据防泄露事件的根源主要集中于内部管理漏洞、技术能力欠缺及运营执行不力等层面。例如，员工权限管理混乱，出现越权访问敏感数据的情况；数据未加密就进行传输，导致数据被窃取；供应链环节存在安全隐患，成为数据泄露的潜在风险点。本文所构建的数据防泄露能力成熟度模型，其能力维度涵盖管理侧、技术侧以及运营侧这3个方面。

（1）管理侧：依托管理规范与标准流程等制度性要求，对数据防泄露全流程防护行为实施刚性约束；

（2）技术侧：通过技术手段和产品工具落实数据防泄露工作要求，自动化实现数据防泄露能力；

（3）运营侧：通过持续的管理过程和技术实践，识别、分析、响应和防范数据泄露风险。

1.4　数据防泄露过程维度

根据电信企业业务性质与运营特点，本文构建的数据防泄露能力成熟度模型将数据防泄露过程分为数据全生命周期过程、业务过程和数据流动过程、通用过程4个维度，每个维度由若干个防泄露过程构成。

（1）数据全生命周期过程维度以数据自身安全为核心，涵盖了从数据产生直至数据被销毁的整个历程，包含数据采集、数据传输、数据存储、数据使用、数据加工、数据提供、数据公开、数据销毁，共15个过程。数据全生命周期过程维度数据防泄露过程如图3所示。

（2）业务过程维度主要聚焦容易引发数据泄

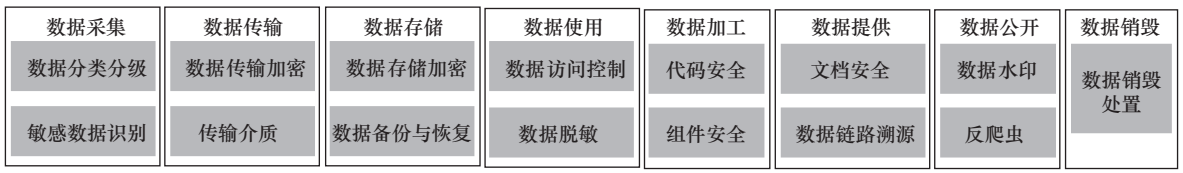

图3　数据全生命周期过程维度数据防泄露过程

露风险的业务环节，包含营销受理、系统运维、客服服务、安装维护、资源开通、大数据，共11个过程。业务过程维度数据防泄露过程如图4所示。

（3）数据流动过程维度主要评估数据从云平台，经传输管道，到终端设备的跨域流动过程中的防泄露能力，包含云侧数据防泄露、管道侧数据防泄露和端侧数据防泄露，共3个过程。数据流动过程维度数据防泄露过程如图5所示。

（4）通用过程维度包含人员管理、账号及权限管理、日志审计、风险监测、数据溯源和应急演练与响应，共6个过程，如图6所示。

1.5　数据防泄露能力成熟度等级

数据防泄露能力的成熟度等级共分为5级，各等级特征见表1。

（1）将每个数据防泄露过程的能力成熟度等级划分为5级，每个等级下的能力要求从管理、技术、运营3个维度进行阐述。

（2）成长级应包含全部3个能力，其他等级可不包含完整的3个关键能力。

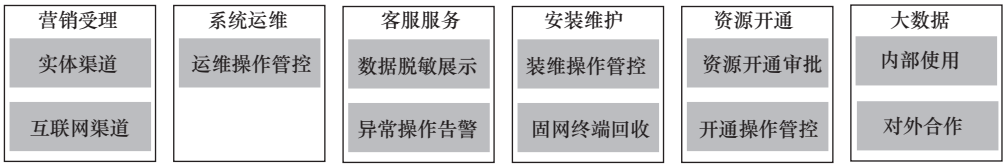

图4　业务过程维度数据防泄露过程

图5　数据流动过程维度数据防泄露过程

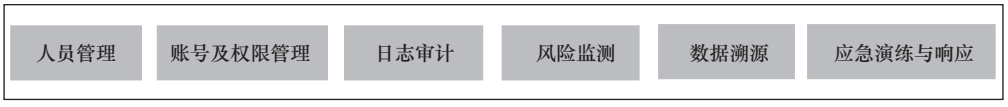

图6　通用过程维度数据防泄露过程

表1　能力成熟度各等级特征

成熟度等级	特征	说明
基础级	在数据防泄露过程中未能有效执行相关工作，仅根据临时工作要求执行相关工作，未形成成熟的机制来保证相关工作的持续有效进行	未制定计划，相关工作无法复制
可管理级	a.对各数据防泄露过程进行规划，提前分配资源和责任，并按照规划开展相关工作； b.对各过程的相关工作进行验证，相关工作按照规划执行； c.若相关工作与规划有重大偏离，能及时对相关工作进行修正	主动、有计划地开展各项工作，但未形成体系
成长级	a.建立数据防泄露工作体系，对各个过程制定标准化的过程文档，相关工作具有标准流程； b.相关工作严格按照制度和流程进行，并记录过程与结果数据，对执行不到位的过程进行核查	建立标准制度、流程，相关工作可重复
先进级	a.制定可量化的目标，用于评判各个过程相关工作的执行情况，并基于量化目标对相关工作进行修正； b.寻找相关工作的改进点，并及时优化	建立可量化的目标，相关工作可度量、可优化
卓越级	a.不断引入新的管理理念、技术趋势和最佳实践，并结合具体业务过程进行验证和优化，再推广至所有数据防泄露过程； b.持续改进各个过程的制度和流程，及时消除缺陷部分，保持数据防泄露能力在行业中的领先地位	引入新的理念和技术，持续优化

（3）对于每个防泄露过程，高等级的能力要求应包含全部的低等级能力要求。

2 评估方法

2.1 制定评估标准

为明确展示不同成熟度等级对数据防泄露过程的能力要求，需提供统一的能力评估框架，因此制定了数据防泄露能力成熟度评估标准。该标准明确界定各成熟度等级下管理、技术、运营能力建设的具体指标与实施路径，为数据防泄露能力评估提供科学、规范的参照体系。由于篇幅限制，仅选取数据流动过程维度中的3个关键防泄露过程，详述其成长级、先进级与卓越级的评估标准，详见表2。

表2 数据流动过程维度成长级、先进级和卓越级评估标准

过程	等级	能力	评估标准
云侧数据防泄露	成长级	管理	a.具备云侧数据防泄露管理规范，明确云侧数据存储、数据隔离、数据访问控制、数据迁移、云安全基线等方面要求； b.明确云桌面等技术工具的使用场景
		技术	a.通过云桌面技术实现云侧数据处理； b.使用技术工具实现云侧敏感数据加密存储； c.使用技术工具（如文件中台系统）实现云侧数据下载、共享、流转，以及审批流程的集中管控
		运营	a.定期检查云桌面等技术工具的使用情况； b.定期开展专项检查，排查网盘、文库、代码仓库等公共平台敏感数据泄露风险； c.使用自动化工具定期扫描安全基线，及时发现问题
	先进级	管理	a.结合数据分类分级策略，明确要求敏感数据和一般数据实施物理或逻辑隔离存储； b.明确云端集约存储策略，要求敏感数据集中存储在经过安全评估和合规认证的自有云平台或指定云服务商的加密专区
		技术	a.利用云侧多租户资源隔离能力，将敏感数据存储在高安全等级的独立数据库实例或专属数据库集群中； b.部署数据库安全网关，将数据库暴露面收敛至单一可控节点
		运营	a.定期利用云侧数据发现与识别工具定位敏感数据，动态调整隔离存储策略； b.定期评估文件中台对云侧文件的纳管覆盖率，以及数据安全网关对数据访问请求的管控覆盖率
	卓越级	管理	密切关注云侧数据防泄露的优秀解决方案，定期审核并调整云侧数据防泄露管理制度
		技术	a.积极参加国际、国家和行业标准的制定，在业界分享最佳实践； b.利用新技术优化云侧数据防泄露技术方案，提升云侧数据防泄露管控能力
管道侧数据防泄露	成长级	管理	a.具备管道侧数据防泄露管理规范，明确数据传输安全要求（如传输通道加密、数据内容加密、身份鉴别、接口管理等）、数据防泄露管理要求等； b.明确数据传输加密的应用场景
		技术	a.通过技术手段实现数据传输加密； b.在网络出口部署网络数据泄露防护系统，对敏感数据传输进行监测； c.部署接口安全网关，提供统一的认证鉴权、流量控制、动态令牌等安全能力
		运营	a.定期检查网络数据泄露防护系统等技术工具的使用情况； b.定期对网络设备开展渗透测试、漏洞扫描、基线核查等安全检测，及时发现隐患并进行加固； c.严格遵循最小权限原则，配置细粒度的接口访问权限策略，启用多因素认证； d.关闭非必要端口（如3389、445等），对业务端口实施IP白名单限制
	先进级	管理	a.明确密钥分段管理要求，严格规范密钥分发审批流程； b.严格遵循国家密码管理局商用密码评估要求，全面采用国密算法
		技术	a.具备异常行为一键阻断能力； b.建立基于机器学习的异常行为分析模型，识别管道侧的数据泄露行为
		运营	定期量化评估管道侧数据泄露风险，分析风险成因，为后续提升数据防泄露能力提供技术支持
	卓越级	管理	定期评估管道侧数据防泄露方案的应用成效及对新风险的应对能力，动态调整控制措施
		技术	a.利用新技术优化管道侧数据防泄露技术方案，提升管道侧数据防泄露管控能力； b.积极参加国际、国家和行业标准的制定，在业界分享最佳实践

续表

过程	等级	能力	评估标准
端侧数据防泄露	成长级	管理	a.具备面向端侧设备的数据防泄露管理规范，明确端侧设备的安全配置管理、数据防泄露管理要求等； b.遵循非必要不落盘的原则，禁止在端侧存储数据，因业务需要确需在端侧存储，应通过审批流程方可实施
		技术	a.打印输出设备应采用身份鉴别、访问控制等手段进行安全管控； b.接入办公网络的终端设备应按统一的要求安装防病毒、终端入侵检测等软件； c.部署端侧数据泄露防护系统，具备敏感数据识别、外发行为管控、剪贴板控制、屏幕水印、操作审计等能力； d.部署文档加密系统，确保端侧文件安全
		运营	a.定期开展端侧操作系统和应用软件的安全补丁更新情况检查； b.定期对员工进行数据安全意识培训，涵盖钓鱼邮件、恶意软件等常见威胁的识别与防范，并普及安全操作规范
	先进级	管理	a.严格控制端侧设备的外设（如U盘、移动硬盘、打印机等）使用权限； b.采用零信任机制，根据用户业务身份自评估结果动态授予网络访问权限
		技术	a.部署数据沙箱，建立工作区与非工作区，限制敏感数据从工作区往非工作区流动； b.建立终端防泄露管理平台，统一纳管端侧数据泄露防护系统，监控数据泄露风险
		运营	a.记录所有传输介质（如U盘、移动硬盘等）插拔事件，对异常拷贝行为进行报警； b.定期对端侧文件加密系统的使用情况开展巡检，统计敏感文件的加密覆盖率； c.对终端防泄露管理平台开展常态化运营，量化评估端侧数据泄露风险，分析风险成因，为后续提升端侧数据防泄露能力提供技术支持
	卓越级	管理	定期评估端侧数据防泄露方案的应用成效及对新风险的应对能力，动态调整控制措施
		技术	a.利用新技术优化端侧数据防泄露技术方案，提升端侧数据防泄露管控能力； b.积极参加国际、国家和行业标准的制定，在业界分享最佳实践

2.2　定级流程

本文根据木桶原理开展电信企业数据防泄露能力成熟度评估，确定最终的能力等级，定级流程如图7所示。

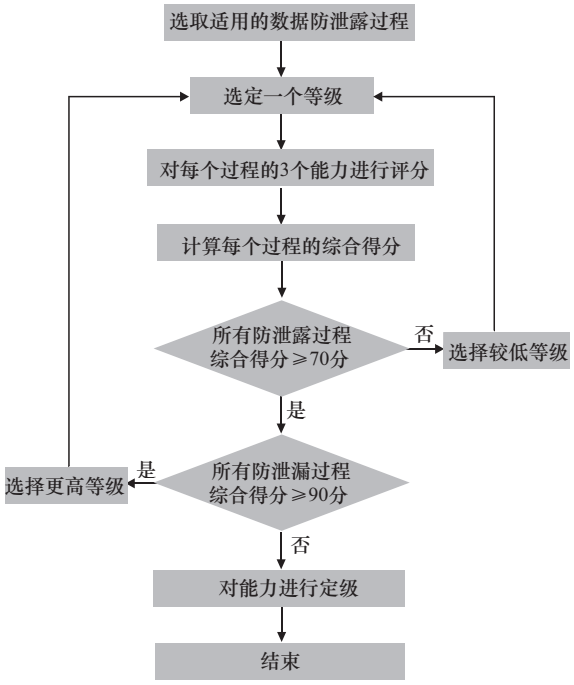

图7　定级流程

首先，被评估的单位根据本单位的实际情况选取适用的数据防泄露过程，再根据能力现状确定目标等级。若部分过程不适用，需提供详实的证明材料，并清晰阐明不适用的具体原因。

其次，评估团队根据该等级对应的评估标准分别对每个数据防泄露过程的管理、技术、运营能力进行评分，并将3项能力得分的加权平均分作为该过程的综合得分。按此方法计算每个过程的综合得分。

然后，根据每个过程的综合得分进行判定，若所有数据防泄露过程的综合得分≥70分，则判定符合该等级，其中，如果所有数据防泄露过程综合得分≥90分，则可申请更高等级评定，每个单位仅有一次升级机会；若存在过程综合得分＜70分，则不符合本等级要求，可选择较低等级重新进行评估。

3　实施评估

为进一步验证本文提出的数据防泄露能力成

熟度评估方法的可行性，本文以中国电信某子公司为例，对其数据流动过程维度数据防泄露能力成熟度进行评估。

集团评估团队依据评估标准，采用人员访谈、文档审核、配置检查、工具测试、旁站式验证等方式，从管理、技术、运营3个能力维度评估其云侧、管道侧和端侧数据防泄露能力成熟度。该子公司的实际情况与评估得分见表3。

在云侧数据防泄露方面，该子公司已制定《云侧数据防泄露管理规范》，明确云侧数据存储、使用等方面的管理要求，制度内容全面。通过部署云桌面、数据安全网关、文件中台等技术工具，实现对云侧数据操作的有效管控。该子公司建立了以90天为周期的常态化运营机制，定期开展多项运营工作，包括云桌面、文件中台、数据安全网关等工具使用情况的巡查、公共平台敏感数据泄露风险排查、安全基线检查以及存储策略优化调整。在管道侧数据防泄露方面，已制定《管道侧数据防泄露管理规范》《数据传输加密管理规范》《密钥管理规范》，明确身份鉴别、传输加密、接口管控与密钥分段管理等要求，并规范密钥分发审批流程。利用基于国密算法的安全传输协议保障数据传输安全，部署网络数据泄露防护系统与接口安全网关管控数据传输及接口调用，借助机器学习算法识别数据泄露风险。建立常态化运营机制，以90天为周期，定期开展各项运营工作，包括安全基线检查、网络数据泄露防护系统和接口安全网关的使用情况核查、优化访问控制策略配置，以及数据泄露风险成因分析。在端侧数据防泄露方面，已制定《端侧数据防泄露管理规范》，明确端侧设备安全基线、端侧数据留存条件、外设使用规则以及网络权限分配等要求。借助防病毒、终端入侵检测等防护软件筑牢端侧设备基础安全防线，部署端侧数据泄露防护系统、文档加密系统、数据沙箱等技术工具，以实现端侧数据全流程安全管控；同时对打印设备采取安全管控措施，防范敏感数据在打印环节外发。每90天定期推进安全基线检查、外设使用情况抽查、文件加密系统使用巡查以及数据泄露风险成因分析工作，每年开展全员端侧数据安全培训，提升人员安全操作能力与风险防范意识。综上所述，参照先进级评估标准，该子公司在云侧、管道侧及端侧数据防泄露过程的综合评分均超过70分，其数据流动过程维度的成熟度等级已达到先进级水平。

该子公司目前尚未建立新兴管理理念、前沿技术及行业最佳实践的定期追踪机制，也未对数据防泄露解决方案开展持续性优化。同时，未积极参与国际标准、国家标准及行业标准的制定工作，缺乏标准话语权。该子公司后续可参照本文提出的卓越级评估标准，全面系统强化数据防泄露能力，持续完善数据防泄露能力体系，从而为企业数据构建全方位、立体化的安全防护屏障。

4 结束语

本文系统梳理了现有文献研究成果，对标数据安全相关政策法规、国家标准及通信行业标准，深度结合中国电信数据防泄露工作实践，构建了一套适用于电信企业落地实施的数据防泄露能力成熟度评估模型。该模型以企业数据防泄露管理实际需求为导向，通过理论与实践的有机融合，为电信行业数据防泄露能力的科学评估与体系化建设提供了可操作的实施框架。

该数据防泄露能力成熟度评估模型采用三维立体架构，由数据防泄露能力、数据防泄露过程、能力等级构成。其中，数据防泄露能力维度从管理要求、技术支撑、运营保障3个层面，系统构建数据防泄露能力评价指标体系；数据防泄露过程维度则深度融合中国电信数据防泄露能力体系实践经验，系统梳理涵盖数据全生命周期、业务、数据流动、通用等环节的35个数据防泄露核心过程。通过能力维度与过程维度的有机结合，辅以能力等级维度的量化分级标准，为电信

表3　某子公司数据流动过程维度数据防泄露能力表现

过程	能力	能力表现	能力评价	得分
云侧数据防泄露	管理	a. 结合数据分类分级策略，编制并发布《云侧数据防泄露管理规范》，内容覆盖全面； b. 明确要求敏感数据加密存储，并和一般数据实施逻辑隔离； c. 推行云端集约存储策略，敏感数据集中存储在自有云平台	a. 符合先进级评估标准，但没有明确要求自有云平台需要经过安全评估和合规认证； b. 缺少两项要求，扣20分	80
	技术	a. 通过云桌面对云侧数据进行操作； b. 将敏感数据存储在专属数据库集群中，并在存储层启用云原生加密，禁止明文存储，访问层实施基于属性的动态授权； c. 数据安全网关作为所有云上数据访问的统一入口，强制要求外部应用通过数据库安全网关连接数据库； d. 已建设文件中台能力，实现对云上文件的统一存储、管理、共享和安全控制	符合先进级评估标准	100
	运营	a. 定期检查云桌面、文件中台、数据安全网关等技术工具的使用情况，评估文件中台对云侧文件的纳管覆盖率，以及数据安全网关对数据访问请求的管控覆盖率； b. 定期排查云盘、文库、代码仓库等公共平台敏感数据泄露风险； c. 定期检查安全基线，及时修补漏洞，更新补丁； d. 定期利用数据识别工具扫描云侧数据，识别敏感数据，及时调整存储策略	a. 符合先进级评估标准，检查周期为90天； b. 检查周期过长，扣15分	85
管道侧数据防泄露	管理	a. 已制定《管道侧数据防泄露管理规范》，明确身份鉴别、接口管控等要求； b. 已制定《数据传输加密管理规范》，细化数据传输加密应用场景，明确使用安全协议传输数据，禁用不安全的加密套件； c. 已制定《密钥管理规范》，明确密钥分段管理要求，严格规范密钥分发审批流程	a. 符合先进级评估标准，但是没有在管理规范中明确要求使用国密算法； b. 缺少一项要求，扣10分	90
	技术	a. 使用基于SM2/SM3/SM4的TLS 1.2安全协议传输数据； b. 已部署网络数据泄露防护系统，实现全流量监测与分析，识别敏感数据，阻断异常传输行为； c. 已部署接口安全网关，对所有接口进行统一管控，具备流量监测、限流、阻断等功能； d. 利用机器学习等算法分析数据传输、接口调用等行为，识别数据泄露风险	符合先进级评估标准	100
	运营	a. 定期对网络设备开展基线检查，包含渗透测试、漏洞扫描、端口管控等； b. 定期检查网络数据泄露防护系统、接口安全网关的使用情况，以及纳管全部数据传输和接口调用行为； c. 实施精细化的接口访问控制策略，并定期优化策略； d. 关闭非必要的端口，实施IP白名单限制； e. 定期分析数据泄露风险的成因，进行闭环管控	a. 符合先进级评估标准，但是检查周期为90天，只分析风险成因，没有量化评估； b. 检查周期过长，扣15分，没有量化评估扣10，总共扣25分	75
端侧数据防泄露	管理	a. 已制定《端侧数据防泄露管理规范》，明确端侧设备安全基线、端侧数据留存、外设（如U盘、移动硬盘、打印机等）使用等要求； b. 采用零信任机制分配网络权限	a. 符合先进级评估标准，但数据留存审批流程不规范； b. 流程不规范，扣20分	80
	技术	a. 对打印输出设备实施严格的安全管控； b. 统一为接入办公网络的端侧设备安装防病毒软件、终端入侵检测软件； c. 端侧设备均部署端侧数据泄露防护系统，并具备敏感数据识别、外发行为管控、剪贴板控制、屏幕水印、操作审计等能力，对敏感数据进行识别、监控和保护； d. 端侧设备均安装文档加密系统； e. 部署数据沙箱，建立工作区与非工作区； f. 具备终端防泄露管理平台，全量纳管端侧数据泄露防护系统	符合先进级评估标准	100
	运营	a. 定期开展端侧设备安全基线检查； b. 定期对员工开展数据安全教育和培训，包括管理要求、技术工具使用和安全运营； c. 记录外设的使用情况，并定期抽查； d. 定期开展文件加密系统使用情况巡检； e. 基于终端防泄露管理平台，量化评估端侧数据泄露风险，并进行闭环管控	a. 符合先进级评估标准，但是检查周期为90天，培训周期为一年； b. 检查周期过长，扣15分；培训周期过长，扣10分，总共扣25分	75

企业精准评估数据防泄露能力水平、优化数据防泄露能力体系提供了科学完备的评价依据与实施路径。本文也存在一定的局限性，未来可以从以下两方面进行改进。

（1）本文虽已针对各数据防泄露过程制定评估标准，但当前评估过程仍主要依赖评估人员的专业经验进行定性评分，缺乏标准化的量化评估工具支撑。

（2）本文构建的评估体系主要基于中国电信数据防泄露实践经验，其防泄露过程维度与评估标准的设定，主要参照通信行业数据安全监管要求与中国电信企业实际业务场景。因此，在医疗、能源、电力等其他行业的适用性方面可能存在一定的局限性。

参考文献：

[1] 徐双, 刘文斌, 李佳龙, 等. 大数据背景下的数据安全治理研究进展[J]. 太原理工大学学报, 2024, 55(1): 127-141.
Xu S, Liu W B, Li J L, et al. Research progress on data security governance under the background of big data[J]. Journal of Taiyuan University of Technology, 2024, 55(1): 127-141.

[2] 裴炳森, 李欣, 樊志杰, 等. 视频监控数据跨域安全共享传输控制系统设计与实现[J]. 信息网络安全, 2024, 24(11): 1721-1730.
Pei B S, Li X, Fan Z J, et al. Design and implementation of a cross-domain secure sharing transmission control system for video surveillance data[J]. Netinfo Security, 2024, 24(11): 1721-1730.

[3] 付爱英, 熊宇峰, 曾勋炜. 同态加密下用户隐私数据传输的安全保护方法[J]. 吉林大学学报(理学版), 2025, 63(2): 573-579.
Fu A Y, Xiong Y F, Zeng Q W. Security protection method for user privacy data transmission under homomorphic encryption[J]. Journal of Jilin University (Science Edition), 2025, 63(2): 573-579.

[4] 李建科. 数据库系统中的数据隐私保护技术分析[J]. 黑龙江科学, 2025, 16(10): 159-161.
Li J K. Analysis of data privacy protection technologies in database systems[J]. Heilongjiang Science, 2025, 16(10): 159-161.

[5] 李晓静, 杨秀杰. 云计算环境下多模态异构网络数据安全存储方法[J]. 现代电子技术, 2025, 48(6): 63-67.
Li X J, Yang X J. Method of secure storage for multimodal heterogeneous network data in cloud computing environment[J]. Modern Electronics Technique, 2025, 48(6): 63-67.

[6] 张晗, 陈立全, 杨波, 等. 5G工业互联网下的轻量级数据使用安全方案[J]. 东南大学学报(自然科学版), 2024, 54(3): 772-780.
Zhang H, Chen L Q, Yang B, et al. Secure lightweight data using scheme in 5G industrial Internet systems[J]. Journal of Southeast University (Natural Science Edition), 2024, 54(3): 772-780.

[7] 籍勇亮, 李松浓, 黄宏程. 云边协同的智能电网数据安全共享方案[J]. 太赫兹科学与电子信息学报, 2025, 23(5): 429-433.
Ji Y L, Li S N, Huang H C. A cloud edge collaborative smart grid data security sharing scheme[J]. Journal of Terahertz Science and Electronic Information Technology, 2025, 23(5): 429-433.

[8] 徐博, 谢江山, 徐晓慧, 等. 云环境中基于联盟链的多中心数据共享系统[J]. 控制工程, 2023, 30(1): 8-17.
Xu B, Xie J S, Xu X H, et al. A consortium blockchain based multi-center data sharing system in cloud environments[J]. Control Engineering of China, 2023, 30(1): 8-17.

[9] 李超, 韩翔, 刘钊, 等. 基于可信计算的跨网数据安全交换技术[J]. 计算机工程与设计, 2021, 42(10): 2762-2769.
Li C, Han X, Liu Z, et al. Data exchange technology across networks based on trusted computing[J]. Computer Engineering and Design, 2021, 42(10): 2762-2769.

[10] 赵丽莉, 王鹏. 公共数据开放中企业数据安全风险及其治理研究[J]. 重庆邮电大学学报(社会科学版), 2025, 37(5): 89-99.
Zhao L L, Wang P. Enterprise data security risks and governance in public data opening[J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2025, 37(5): 89-99.

[11] 杨尚东. 论大数据时代政府信息公开中的敏感个人信息保护[J]. 行政法学研究, 2025(4): 101-114.
Yang S D. On the protection of sensitive personal information in government information disclosure in the big data era[J]. Administrative Law Review, 2025(4): 101-114.

[12] 张星, 张兴, 王晴阳. DP-IMKP: 满足个性化差分隐私的数据发布保护方法[J]. 计算机工程与应用, 2023, 59(10): 288-298.
Zhang X, Zhang X, Wang Q Y. DP-IMKP: data publishing protection method for personalized differential privacy[J]. Computer Engineering and Applications, 2023, 59(10): 288-298.

[13] 韩春花, 许海云, 孙杰, 等. 数据生态视角下科研大数据治理成熟度模型构建与评估研究[J]. 情报理论与实践, 2025, 48(4): 22-34.
Han C H, Xu H Y, Sun J, et al. Research on model building and evaluation of governance maturity of scientific research big

data from the perspective of data ecology[J]. Information Studies (Theory & Application), 2025, 48(4): 22-34.

[14] 程越, 王双. 资产管理数字化成熟度模型构建与应用[J]. 科技管理研究, 2024, 44(19): 50-62.
Cheng Y, Wang S. Construction and application of maturity model for digitalization of asset management[J]. Science and Technology Management Research, 2024, 44(19): 50-62.

[15] 袁静, 刘晓媛, 王思君. 政府数据开放平台成熟度评估指标构建及实证研究[J]. 图书馆建设, 2025(4): 84-98.
Yuan J, Liu X Y, Wang S J. Construction and empirical study of maturity evaluation indicators for open government data platforms[J]. Library Development, 2025(4): 84-98.

[16] 林杰, 姜天晗. 企业管理信息系统的数据安全治理能力成熟度模型研究[J]. 上海管理科学, 2025, 47(2): 32-42.
Lin J, Jiang T H. Maturity model of data security governance capability for enterprise management information system[J]. Shanghai Management Science, 2025, 47(2): 32-42.

[17] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型[S].
GB/T 37988—2019Information security technology—Data security capability maturity model[S].

[作者简介]

王雪琼（1987– ），女，中国电信股份有限公司研究院工程师，主要研究方向为数据安全体系规划、数据安全技术等。

刘坚桥（1993– ），男，现就职于中国电信股份有限公司江西分公司，主要研究方向为通信领域网络安全运营、数据安全治理等。

周旭华（1983– ），男，博士，中国电信股份有限公司研究院高级工程师、数智安全研究中心副总监，主要研究方向为数据安全技术、密码技术等。