ISSN：3078-8994
EISSN：3104-4492

数据分级分类与供应链安全融合等级保护测评落地研究

穆琛伟

联通数字科技有限公司，北京 100031

摘　要：数字化转型趋势下，数据成为组织运行和价值创造的重要资源。供应链协同模式的广泛采用进一步推动了数据在跨主体、跨平台、跨业务场景流动与共享，数据安全风险呈现链条化、关联化和扩散化特征。传统等保测评侧重于网络和系统安全保护，难以满足数据要素流通环境下的治理需求。文章结合数据分级分类发展趋势和供应链安全融合发展趋势，分析两者与等级保护测评之间存在的关联性问题，并探讨供应链环境下数据流转风险、权限控制逻辑及风险传导机制，在此基础上构建以数据等级为核心、以供应链节点为抓手、以闭环治理为导向的等级保护测评落地框架，为数据安全治理与等级保护制度协同实施提供参考借鉴。

关键词：数据分级分类；供应链安全；等级保护测评；数据安全治理；风险控制

DOI：10.64649/yh.shfzykjcx.issn3078-8994.202607013

0 引言

随着数据要素价值持续释放，组织间业务协作深度不断提升，数据处理活动逐渐突破传统组织边界，并沿供应链体系向研发、采购、运维、服务和管理等多个环节延伸[1]。数据流转范围扩大带来业务效率提升，也使数据泄露、权限滥用、第三方风险传导等问题日益突出。等级保护制度作为网络安全管理的重要基础，在保障信息系统安全运行方面发挥着重要作用，但面对数据分类分级管理要求和供应链安全治理需求，其实施路径亟须进一步细化。基于此，文章从数据分级分类与供应链安全协同治理视角出发，围绕风险识别、控制逻辑与落地机制展开研究，探索等级保护测评与数据安全治理深度融合的实现路径。

1 数据分级分类与等级保护测评协同落地的理论基础

1.1 数据资产识别与安全边界重构

数据分级分类与等保落地的前提，是对数据资产进行可识别、可描述、可追溯梳理，将原本零散的业务记录和日志转变为权属、流向、价值和风险属性明确的治理对象，重构安全边界[2]。与传统等保侧重系统、网络、设备和应用相比，保护的重心放在了数据本身上，安全边界由物理或系统范围扩展到采集、存储、使用、共享、传输与删除的生命周期。在数据资产识别中，不仅仅是目录登记，更主要是融合业务功能与敏感性为等保测评提供依据。

1.2 分级分类规则与保护要求映射

分级分类规则的制度价值，就是将抽象的数据安全要求转化为可执行、可评估的保护措施，同时在等级保护中与控制要求实现对应。依据业务属性、处理场景和管理责任进行分类，而数据分级侧重于泄露、篡改或非法利用对国家安全、公共利益以及权益带来影响，二者结合形成反映业务差异和风险强弱的治理尺度[3]。在等级保护测评中，需要把分级分类结果与身份鉴别、访问控制、安全审计、边界防护、数据备份、加密保护以及接口管理这些控制项相对应，使不同等级数据获得对应的保护强度，避免平均化会出现资源错配和敏感数据低强度处理情况。

1.3 等级保护测评指标体系下的数据安全责任嵌入

等级保护测评指标体系为数据安全治理提供制度化、程序化和技术化的评价框架，而要推动数据分级分类落地，就必须将数据安全责任嵌入到组织管理、人员管理、系统建设、运行维护与供应链协作中。责任嵌入并非仅对某个部门进行职责明确，其过程是由各数据所有者、管理者、使用者、运维者以及外部服务提供方围绕数据等级、权限、操作记录和风险处置形成可衔接的责任链条。等级保护测评关注制度、措施、记录与风险闭环；数据分级分类则需要将责任配置适应数据敏感程度，在审批授权、访问留痕、外发控制以及接口调用等环节，相关操作均受到更加严格的约束，以此让数据安全责任成为等级保护测评运行的内在支撑。

2 供应链安全风险传导机制与数据保护耦合逻辑

2.1 供应链主体关系中的数据流转风险识别

供应链环境下的数据流转并不仅仅局限在

ISSN：3078-8994
EISSN：3104-4492

单一组织内部调用、处理业务，而是伴随研发协同、采购管理、运维支撑、平台接入、外包服务、设备交付等关系在不同主体之间、不同系统之间和不同权限边界之间存在着流动，因而其风险传导结构较为复杂。将数据分级分类嵌入供应链安全治理中后需要将数据流向、接触主体、处理目的、存储位置、接口调用频次与业务依赖程度纳入识别范围，判断何种类型数据暴露于哪些节点、哪些环节、哪些权限条件下。

2023 年，广泛应用于政府、金融、医疗等领域的 MOVEit 文件传输软件被发现存在高危漏洞，攻击者利用该漏洞从众多组织的数据交换链路中非法获取敏感信息，受影响机构超过 2500 家，暴露出第三方数据传输平台成为风险放大节点的现实问题。该事件表明，即便组织自身安全防护体系较为完善，只要供应链环节中的服务提供方或数据交换平台存在缺陷，风险仍可沿着数据流转路径向关联主体扩散。

如果供应链各主体仅依据合同关系或自身应承担的安全责任，就很难考虑数据在委托处理、远程维护、组件适配、日志回传、漏洞处置的实际流动状态；较为严谨的识别路径则需以数据生命周期为线索，将相对重要的数据、个人信息和业务敏感信息纳入视域，面向主体关系、技术链路与管理责任。

2.2 外部协作场景下的数据权限与信任控制

在外部协作的场景下，数据保护由组织内控到多主体联合治理中的权限配置和信任控制是供应链安全与数据分级分类耦合的重要环节。如供应商、集成商、运维服务商、云服务商以及检测机构等人员在履职过程中可能会接触系统配置、接口文档、运行日志或者业务数据等信息，若授权边界没有设定好等级规范，就可能会出现越权访问和数据失控风险。利用分级分类结果进行权限治理时，应当坚持最小必要、用途限定、动态校验和操作留痕原则，将数据等级与账号权限、访问时间段、操作范围以及审计策略相关联，并对外部主体的真实性和行为可追溯性加以约束，使得信任成为了等级保护测评中可检查、可验证的控制对象。

2.3 供应链风险向等级保护测评控制项的转化路径

供应链风险纳入等级保护测评的关键，在于将外部依赖、数据接触、组件引入和服务交付分散的风险转化为可描述、可取证与可判定的安全控制要求。由于数据分级分类是确立风险转化尺度的前提条件，不同等级数据在具体供应链场景下所需满足的等级保护要求落实到相应的安全管理制度、人员管理、系统建设、供应商选择、外包运维、访问控制以及安全审计等方面[4]。对于高等级数据相关的供应链节点来说，从资质审查逐步延伸至远程接入、权限审批、数据脱敏、接口日志、第三方管理以及退出机制等环节，使得供应链风险能够由外部不确定性转换成各方责任项和证据项，数据保护要求做到闭合并且具有操作性。

3 数据分级分类与供应链安全融合的等级保护测评落地机制

3.1 以数据等级为核心的安全控制基线构建

数据分级分类与供应链安全融合进入等级保护测评实施阶段，需要结合数据等级的不同打造差异化安全控制基线，将数据价值、敏感程度、流转范围和风险影响与对应的等级保护控制要求相匹配，而非仅按照系统等级提出安全措施。在具体操作过程中，应当建立“数据等级—等级保护控制点—供应链审查要求”映射关系，将数据的分类和分级结果与身份鉴别、访问控制、安全审计、数据完整性、通信保护等控制要求相衔接，并根据供应链节点职责、数据接触范围和业务场景对其进行差异化管理；对于处于不同等级的数据，应从访问授权、传输保护、接口调用、日志审计以及供应商管理等方面采取与风险水平适宜的安全控制措施，形成覆盖数据全生命周期和供应链全过程的安全控制基线。典型映射关系如表 1 所示。

表1 数据等级与等级保护控制要求映射示例

数据场景	等级保护重点控制点	差异化控制措施	供应链审查重点
二级系统一般业务数据	身份鉴别、访问控制	普通账号认证、权限分配、日志留存	检查供应商账号权限是否按岗位配置
二级系统重要业务数据	身份鉴别、安全审计、数据完整性	重要操作审批、完整性校验、共享审批	检查数据处理流程、备份恢复及日志留存
三级系统重要数据	身份鉴别、访问控制、通信保护、安全审计	多因素认证、最小权限、传输加密、全过程审计	检查远程运维、接口调用、数据脱敏、权限审批
三级系统核心数据	访问控制、数据完整性、安全审计、集中管控	全生命周期保护、严格外发审批、持续监测	检查供应商安全能力、关键岗位管理、组件安全验证、退出阶段数据删除与权限注销

ISSN：3078-8994
EISSN：3104-4492

由表 1 可见，随着数据等级和等级保护对象保护等级的提高，控制重点逐渐从基础的身份鉴别、访问控制扩展到通信保护、数据完整性、安全审计、全过程管理等多个控制点；供应链安全审查内容也由以往针对供应商资质进行审核延伸至远程运维、接口管理、数据脱敏、退出管理等全过程管理要求。通过建立上述映射关系，能够使得数据分类分级结果直接对应等级保护测评控制项，实现控制措施可配置，检查内容可量化，整改要求可落实，有效提升等级保护测评实施效果。

3.2 以供应链节点为抓手的全过程审查机制

供应链节点审查是数据分级分类要求进入等级保护测评实践的重要承载，其重点不能仅停留在合作前资质审核，而应覆盖供应商准入、系统接入、权限开通、服务实施、变更管理、交付验收、退出清理等全过程 [5]。在准入阶段，应围绕外部主体安全管理能力、数据处理能力、合规记录和技术保障条件开展审查，并以可接触的数据等级确定审查深度；在履约阶段，将账号授权、远程运维、接口开放、数据调取、日志回传、补丁更新、组件替换等行为纳入持续监督。2020 年 SolarWinds 供应链攻击事件表明，供应链风险不仅存在于准入阶段，还可能贯穿软件开发、版本更新、产品交付和运行维护全过程。应在版本变更、系统升级、权限调整等关键节点建立动态评估机制，并核验退出阶段的数据删除、权限注销及介质回收等情况，使等级保护测评能够围绕供应链全周期形成完整证据链，验证数据保护措施是否真正落实到业务协作过程。

3.3 以闭环治理为导向的持续改进与合规固化

等级保护测评落地不是一次性活动的结束，而是数据分级分类和供应链安全融合治理进入稳定运行后不断校正中的，闭环治理要把发现问题、风险评估、整改落实、复核验证、制度更新和责任追踪作为统一链条。围绕数据等级变化、系统调整、供应商更替以及接口扩展建立常态化的复核机制，使得分级分类结果与安全控制基线、供应链要求保持一致；针对高等级数据保护水平低、第三方权限弱、审计缺失和数据外发审批不严等情况，明确整改的责任、时间和验证方式，防止将风险停留在文档层面，并通过合规固化将整改转化为制度、流程、技术配置，让数据保护从阶段性响应变为日常运行规则，同时也成为可核验的测评依据。

4 结论

数据分级分类、供应链安全治理与等级保护测评并非是彼此独立的管理单元，而是在数据要素流通下相互联系、相互支撑的治理单元。数据分级分类有助于为安全资源配置提供依据；供应链安全治理拓展了风险管理边界，等级保护测评能够为制度落实和控制验证提供评价框架。文章围绕理论基础、风险传导机制与落地路径进行研究，并提出以数据等级为导向形成控制基线、以供应链节点开展全过程审查、以闭环治理强化持续管控的实践思路，将数据安全要求嵌入到供应链运行过程中，推动安全管理、合规要求和业务发展协同统一。

参考文献：

[1] 张茜雅 . 解读《网络数据安全管理条例》[J]. 北京档案 ,2025, (7):36-40.

[2] 全国网络安全标准化技术委员会 (SAC/TC 260). 数据安全技术　数据分类分级规则 :GB/T 43697-2024[S]. 中国标准出版社 ,2024.

[3] 孙瑜晨 , 郑诗彦 . 开放共享为导向的科学数据分类分级制度建构：价值旨归与实现路径 [J]. 科技进步与对策 ,2025,42 (12):140-150.

[4] 刘井强 , 田星 , 舒钰淇 , 等 . 大模型赋能软件供应链开发环节安全研究综述 [J]. 信息安全学报 ,2024,9 (5):87-109.

[5] Okafor C , Schorlemmer T R , Torres-Arias S ,et al.SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties[J]. 2024.

作者简介：穆琛伟（1999.03—），男，汉族，陕西西安人，本科，初级工程师，研究方向：网络安全。