企业信息系统用户权限管理常见问题与优化路径

张一丹　阮崧旭

1.云南省昭通市五华区昌源中路 139 号 6 幢 1 单元 201 云南 昭通 657000

2.云南省昭通市昭阳区小石桥巷 31 号附 41 号 云南 昭通 657000

【摘　要】：企业数字化转型不断深入的时候，信息系统成了企业日常经营、业务管控、数据流转的主要载体，用户权限管理是保证信息系统安全稳定运行、防范内部数据风险、落实内控合规要求的重要环节。目前大多数企业信息系统用户权限管理存在着配置粗放、管控脱节、监督缺位等诸多问题，既影响业务运转效率，又埋下数据泄露、违规操作、内控失效等安全隐患。本文根据企业信息系统运维和管理实际经验，对目前存在的用户权限管理问题进行梳理，并分析问题产生的原因，最后提出相应的优化路径，帮助企业建立规范、高效、安全的权限管理体系，为企业数字化运营筑牢安全防线。

【关键词】：企业信息系统；用户权限管理；内控合规；数据安全

DOI:10.12417/2705-0998.26.05.002

1 引言

伴随着企业信息化建设的不断深入，ERP、OA、CRM、财务核算、生产管理等各种专业信息系统已经全面覆盖到企业的业务流程，系统内部保存着企业核心经营数据、客户信息、财务机密、技术资料等重要资源，用户的权限直接影响到员工对系统资源的访问、操作、修改和导出的范围。科学完备的用户权限管理可以做到权责分明、操作有迹可循，既保证了员工正常的业务开展，又防止了越权操作、数据泄露等隐患，相反若权限混乱、管理无序，则容易造成业务操作的权责不清，从而加大内部控制的风险，并且还会影响企业的正常经营秩序。目前部分企业对于信息系统用户权限管理重视不够，管理模式粗放、流程机制缺失、技术支撑薄弱，各种权限管理问题层出不穷，是企业信息化管理和内控风控的薄弱环节。因此，对企业的信息系统用户权限管理共性问题进行梳理，并提出相应的优化路径，对于提高企业信息化管理水平、保证数据资产的安全、推动内控合规落地有着十分重要的现实意义。

2 企业信息系统用户权限管理常见问题

2.1 权限配置粗放，权责匹配度严重不足

大多数企业还没有形成标准的权限配置体系，权限分配没有统一的标准，大多采用粗放式的、经验化的配置方式，主要存在权限冗余和权限缺失两个问题。一方面，部分企业为了提高业务办理的便利性，给员工过多地分配了系统的权限，导致出现一人多权、跨岗权限、冗余权限等问题，使得普通岗位的员工可以访问到核心财务数据、管理层权限、技术后台资源等，越权操作、数据泄露的风险大大增加；另一方面，部分企业权限配置过于僵化，没有根据岗位的实际需要准确地划分权限，员工因为权限不足而不能完成自己的本职工作，经常向管理层申请权限的调整，增加了运维的工作量，也降低了业务的运转速度。

2.2 权限全生命周期管理缺位，动态管控完全失效

用户权限管理是贯穿员工入职、在岗、调岗、离职全过程的动态工作，但是大多数企业只重视入职初期的权限开通，忽略后续的动态调整，造成权限管理的断点盲区。员工岗位调动、职责变更之后，原有的岗位权限没有及时收回，新增加的岗位权限叠加配置，长时间累积下来就形成了权限臃肿，员工持有大量与当前岗位无关的闲置权限；员工离职之后，系统账号和对应的权限没有及时冻结、注销，造成僵尸账号和僵尸权限的存在，成为外部入侵、内部数据窃取的隐形通道。

2.3 多系统权限割裂，形成跨平台管控孤岛

大型企业普遍存在着多系统并行运行的现象，各个业务部门所辖的信息系统分别由不同的部门来管理，系统的架构以及权限控制模式彼此之间存在差异，没有创建起一个统一的权限管理平台，从而形成了典型的权限孤岛。员工入职后需要在各个系统上分别创建账号和权限，调岗、离职时管理员需要逐个登录各个系统进行权限的调整，操作过程繁杂，容易造成遗漏配置或者错误配置。另外不同系统的权限控制标准不一样，角色定义、权限粒度划分差别很大，同一个员工在不同的系统中所拥有的权限范围没有被协同管控起来，企业不能对全局权限进行统一的排查、管控和审计，整体权限管控力度大大降低，也加大了跨系统数据安全风险。

2.4 审计监督与追责机制不完善，管控约束力不足

部分企业没有形成常态化的权限审计机制，缺少专业的审计工具和流程，不能对系统内冗余权限、僵尸权限、越权权限进行定期排查，权限管理问题长期存在而不能被发现。即使进行权限审计，也是以人工抽查为主，覆盖面小、效率低，不能对全系统的权限配置及使用情况有全面的了解。企业缺少完善的权限操作追溯和追责机制，系统内权限操作日志记录不完整，员工越权操作、违规使用权限之后，不能迅速找到责任人并追踪操作过程，对于权限管理失职、违规授权等行为也没有

相应的追责条款，内控部门和运维部门没有管控约束力，造成权限管理问题反复发生，难以形成长效管控效果。

3 企业信息系统用户权限管理优化路径

3.1 构建精细化权限配置体系，落实最小权限原则

优化权限管理的关键在于打破粗放式配置模式，严格实行最小权限原则，创建起与岗位职责相契合的标准化权限体系。企业要对各部门、各岗位的工作职责、业务流程和系统操作需求进行全方位的梳理，确定每一个岗位所必须的操作权限以及不能够操作的权限，划分出权限管控的等级，把系统的权限分成基础查询、日常操作、核心管理和后台运维这四个等级，从而达到权限粒度精细化拆分的目的。其次，创建标准化岗位权限模板，依照岗位类别制订统一的权限配置准则，给每个岗位的员工统一发放模板来开通权限，防止主观随意地进行配置；对特殊岗位以及临时业务情况下的权限申请流程加以制定，确定临时权限的使用范围和有效期限，到期后会自动收回，防止出现临时权限长期保留的情况。最后创建权限配置复核机制，运维部门完成权限开通之后，联合业务部门、内控部门展开双重复核，保证权限配置同岗位需求完全契合，从源头上防止出现权限冗余或者缺失的情况。

3.2 完善全生命周期管控流程，实现权限动态闭环管理

就权限管理断点而言，创建起包含员工全部职业阶段的权限动态管控流程，从而达成权限开通、变更、收回、注销等环节的全面闭环。入职环节，员工权限开通要经过部门申请、人事审核、运维配置、内控复核四个程序，不得私自开通权限，在岗环节，员工岗位变动、职责调整时，业务部门应立即提出权限变更申请，运维部门同步收回原权限并开通新权限，实现权责同步调整，离职环节，人事部门提前将离职人员信息发送到运维部门，运维部门在员工离职当天全部完成系统账号的冻结和权限注销工作，形成交接确认记录，防止出现僵尸权限。

图 1 全生命周期管控体系

3.3 搭建统一权限管控平台，破除跨系统权限孤岛

针对多系统权限割裂问题，企业要整合已有的信息系统资源，创建起统一的用户权限管控平台，从而达成跨系统账号和权限的集中治理以及协同管控。统一平台具有账号集中创建、权限集中配置、批量调整、统一注销等主要功能，员工使用统一身份认证登录各个业务系统，不需要重复创建账号，管理员在单一平台上可以完成整个系统的权限管控操作，大大提高管理效率，降低配置失误的风险。在统一平台上制定出全局权限管控标准，统一各个系统的角色定义以及权限划分规则，达到全局权限实时监控、统一排查的目的，打破各个系统之间的管控壁垒。企业根据自身的信息化水平，有计划地将统一平台同各个业务系统进行深度对接，达到权限数据实时同步、自动更新的目的，从而加强动态管控能力。

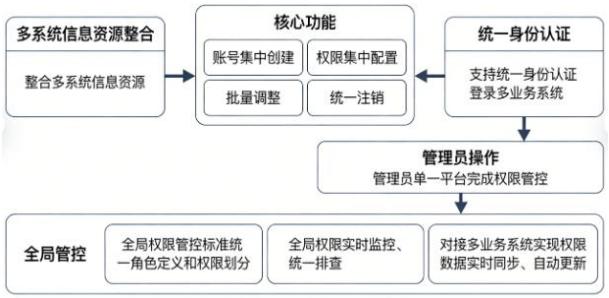

图 2 统一权限管控平台

3.4 健全审计监督与追责机制，强化管控刚性约束

创建常态化的、全方位的权限审计体系，采用信息化审计手段，定时对整个系统权限进行全方位的检查，重点对冗余权限、僵尸权限、越权权限进行细致的核验工作，形成审计报告，并要求责任单位在规定的时间内完成整改，审计周期可以按照季度来安排，主要系统可以在月度内完成。完善系统操作日志管理，对权限开通、变更、回收以及员工系统操作全过程进行详细的记录，保证每一个权限操作、业务操作都有迹可循、可以核查。在此基础上制定出明确的权限管理追责制度，对违规授权、私自调整权限、越权操作等行为进行分类，确定相应的处罚措施，把权限管理纳入到部门和员工的绩效考核体系当中。内控部门对审计整改和追责落实情况进行全过程监督，保证审计发现问题全部整改到位，形成排查、整改、监督、追责的闭环。

3.5 强化全员权限管理素养，夯实管理基础

权限管理不单是运维和内控部门的工作，也是全员的配合工作。企业要定期组织信息系统权限管理培训，对管理层、业务部门员工、运维人员进行权限管理的重要意义、制度规范、操作要求的培训，明确越权操作、违规使用权限的风险及后果，提高全员合规操作意识。对运维人员进行专业的技能培训，提高运维人员对于权限配置、平台运维、风险排查等各方面的能力，对业务部门员工进行相关的权限申请、使用、报备流程培训，杜绝业务部门员工私自提报权限需求，营造全员重视、全员遵守的良好的管理环境。

4 案例分析

4.1 案例企业权限管理现存问题

该企业的前期权限管理问题与前面总结出的共性问题十分吻合，一是权限配置过于粗放，没有按照岗位设置权限模板，销售岗员工可以随意查看生产技术数据，财务岗权限叠加过多审核权限，冗余权限占比超过三成，部分基层员工因为缺少权限而不能完成日常单据提交，业务效率低下。二是缺少全生命周期管控，近一年内离职的有 26 人，其中 11 人的账号权限没有及时注销，造成僵尸账号；15 名调岗员工原有的权限没有收回，新的权限直接叠加，权限臃肿现象严重。第三，多系统权限割裂，五个系统分别由不同的部门来管理，管理员需要登录各个系统才能进行操作，权限的变更非常麻烦，经常会出现遗漏整改的情况。四、审计监督缺位，只在每年做一次人工权限核查，不能及时发现违规权限，操作日志记录不全，数据异常后不能追查责任人。

4.2 针对性优化整改措施

企业根据自身业务特点，严格按照本文提出的方法对整改路径进行推进，首先整理出 32 个核心岗位，建立标准化权限模板，实行最小权限原则，将权限划分为不同的等级，规定各个岗位可以访问的系统模块和操作范围，对于特殊的临时性权限设置 7 天的使用期限，到期后自动收回。其次创建全流程权限管控体系，联系人事、业务、运维、内控四个部门，创建起入职开通、调岗变更、离职注销的闭环流程，人事部门即时把人员异动信息传送给运维部门，运维部门限时完成权限变动工作，内控部门全程审核。另外整合现有的系统资源，创建简易统一的权限控制平台，对五个系统账号和权限进行集中管理，统一身份认证入口，简化管理员的操作流程。最后创建起季度权限审计机制，开启系统全操作日志记录，明晰权限管理追责规定，把合规情况纳入到部门绩效考核当中。

4.3 整改实施成效

经过六个月的整改优化，该企业的权限管理乱象得到了彻底的整治，共清理出冗余权限、僵尸权限 420 多项，权限配置的精准度大大提高，业务部门权限申请的次数减少了 60%，管理员日常运维的工作量也大大降低了一半以上。多系统集中管控之后，权限调整速度提高 80%，没有再出现离职员工权限没有注销、调岗员工权限叠加的情况。常态化审计机制得以建立之后，对于可能存在的违规权限做了及时的排查与整改，所有的系统操作都有迹可循，再也没有出现数据泄露、违规操作等安全事件，内控合规水平得到明显提高，既能保证业务的高效运转，又能构建起企业核心数据资产的安全防线。

5 结论

企业信息系统用户权限管理是一项系统性、长期性的工程，它同企业的数据资产安全、内控合规的落实以及数字化运营的高效有着直接的关系。目前企业存在的权限配置粗放、生命周期管控缺失、跨系统孤岛、审计监督薄弱等问题，本质上都是由于管理理念、流程机制和技术支撑三者同时存在缺失所导致的。企业要改变粗放式管理思想，把最小权限作为核心原则，从标准化体系创建、全流程闭环控制、统一平台搭建、审计追责加强、全员素质提高这五个方面入手，塑造起规范、高效、安全的权限管理体系。同时企业还要根据自身业务的发展以及信息化升级的需求来不断改善权限管理方式，对权限进行动态的调整，并且对权限的管控流程进行不断的改进，使得权限管理一直符合企业经营发展的需要，保证业务运转的便捷性的同时，也筑牢了信息系统和数据资产的安全防线，为企业的数字化转型和高质量发展奠定基础。

参考文献：

[1] 彭思喜,彭鹏.基于双角色权限控制的 B/S 结构管理信息系统安全机制[J].汕头大学学报(自然科学版),2020,35(02):47-53.

[2] 古扎努尔·艾合买提.管理信息系统中用户权限管理实现方法探析[J].信息系统工程,2019,(06):54.

[3] 万骏炜.企业信息系统用户管理功能设计研究[J].海峡科技与产业,2019,(06):136-137+142.

[4] 吕华辉,林志达,梁志宏.企业级信息系统身份权限统一管理研究与应用[J].电子世界,2019,(08):88-89.

[5] 王延昭,张晓祥,奈存剑,等.医院信息系统分级授权管理机制的研究和设计[J].中国医院管理,2016,36(03):54-55.