ERP系统中用户权限的设置规范与控制策略

张有峰（教授）

【摘要】ERP系统中，对于用户权限的管理与控制，既需将其与会计规范及企业内部控制要求的落实密切结合，又需在用户授权、密码控制、操作监控、参数约束等系统操控进程中予以针对性关注。有效分配财务会计人员职权，并要求用户按规范要求使用与维护所拥有的权限，这是会计信息系统正常运行的前提，也是ERP系统安全运作的保障。

【关键词】ERP系统；用户权限；密码；控制策略

【中图分类号】F232　　【文献标识码】A　　【文章编号】1004-0994(2017)10-0067-4

在ERP系统中，财务子系统的每一次运作都可能触及企业运营与发展最为核心的数据。在信息化水平持续提高、企业信息保护意识普遍增强这一背景下，软件开发者与使用者都更加重视对会计信息滋扰因素的防护，监管部门也更加重视对违规、舞弊现象及其滋生环境的防控。如今，多种预防措施以及多方位的权限控制技术，在提高财务数据安全性的同时，也增强了信息系统的规范性。

一、用户权限控制的几种方式

为保护用户数据的安全，软件开发者利用多种形式的配置方式和植入手段，为用户提供多层次的权限管理与操作控制功能。这些功能或以权限设置方式明示于用户，或以参数设置与权限牵制规则隐含于软件内置操控规范中。多层次的控制措施为不同用户营造出相对安全的个性化的应用空间。

1. *密码设防与控制*。财务系统中的密码有两种类型：一种是由操作员个人拥有的身份密码，作为登录软件的通行码，操作密码是用户合法身份和操作权检验工具；另一种是针对某一具体功能或环节设置的权限码，这种密码作为启用某项操作功能或进入某一操作环节的口令，可以被多个用户同时拥有，例如个别软件为反过账和反结账所设置的开启密码就属这一类。密码控制阻止了可能实施的针对会计业务的非规范操作行为，有效地保护了账套数据的安全。

2. *授权与动态管辖*。ERP系统管理员掌管所有操作员的权限，可对操作员进行增加、删除、授权等操作，也可对用户操作权限的使用范围、行使条件等进行具体的设定。在信息化系统中，授权与权限管辖是软件层面保障数据安全的又一重要措施。

3. *用户身份限制*。从权限角度来看，用户区分为两种类型：一类是拥有软件环境控制或账套重要参数设置权限的超级用户，实务中也按是否具有实质性业务处理权限而区分为系统管理员与账套主管；另一类是具有软件的全部或部分业务处理权限的普通用户。身份与权限的对应关系通常在软件开发环节就已确定，并将这一关系固化在程序中。有的软件运用分组管理或角色管理方式，将用户纳入不同的用户组，再通过对用户组属性定义来划分用户的身份。

4. *系统参数约束*。ERP系统为财务活动的每一环节预置了与核算内容及作业流程直接相关的一整套选项参数。例如，存货核算选项使操作员只能应用设定范围内的方法进行商品计价。丰富的环境参数及灵活的定义方式，使系统在调整或限制某些业务处理功能的同时，也限制或屏蔽了用户的操作权限。

5. *软件内在规范制约*。财务子系统服务于会计业务，同时也受到财务会计相关制度规范的约束，会计的钱账分管、内部控制、稽核等制度直接体现于软件的操作控制与权限制约之中。这些控制可能表现为对输入内容的逻辑检验，对重要数据或核心业务环节的操作限制，或者对折旧计提、费用结转等典型业务的标准化处理步骤的设定。这使操作员的权限被限定于软件所允许的操作规则与实施范围之中，

任何情况下，任何用户都无法突破软件开发环节所设定的财务会计规范的制约。

二、用户权限控制原则及其操作策略

用户操作权限控制是软件权限管理与控制的核心，拥有必要的操作权限也是会计人员完成专业工作的前提。

1. *用户操作权限的设置类别*。用户操作权限体现为对软件功能的应用权限，但不限于针对软件功能项目的操作权。有些软件允许或要求管理员设置用户的权限适用范围，也有的软件允许设置特定用户的科目、金额权限范围，以实现对用户权限的精细划分。通常情况下，用户的权限涉及以下几个方面：

（1）项目权限。即确立用户是否拥有对软件具体功能项目的操作权限，这是最基本的权限定义内容。一般来说，权限项目划分越细，权限分配的灵活性越大，可实现对操作权限与内部分工的精确控制。通用软件一般将全部模块的所有权限项目归集在一个窗口界面中，在此可对用户就任一模块的任一操作项目授权。在用友软件中，账套主管可在本账套范围内，就科目、用户表、工资项目、仓库等门类进行具体分解，实现对操作员权限的立体式定义；而在金蝶软件中，系统设置了一项名为“检查科目权限”的控制开关，以便必要时开启或关闭特定用户的科目权限，如下图所示：

金蝶软件的用户权限设置

（2）范围权限。一般情况下，用户所拥有的权限是针对某一账套的，所以，权限被限制在软件中的一个账套范围内，多数软件遵循这种权限与账套间的对应关系。部分软件对权限范围的划分更为详细，管理员授权时可以设定用户在一个账套内的权限作用范围，前述对用户以分组方式或角色定义方式来框定权限范围就是比较典型的做法。在金蝶软件中，用户的权限作用范围有当前用户、本组用户和所有用户三个级别。

（3）金额权限。所谓金额权限是指用户能够处理的会计业务的金额范围，通常是指用户有权处理的最大金额。金额权限既与企业规模相适应，又与用户所任岗位或职务相联系。一些岗位结构复杂、业务量大的企业，常采用分层管理与分级控制的方法来实现对不同职位人员权责的差别管理，这时，金额控制手段就非常有用了。在用友软件中，账套主管通过总账设置菜单中的“金额权限分配”项来履行金额权限管理职能。

2. *权限控制的原则*。控制用户权限的目的是约束操作权限，保护账套数据的安全。如果权限设置不当，不仅违反会计工作规范，还会降低信息系统的运行效率。为此，操作权限控制应掌握以下原则：

（1）遵循内部控制制度。权限设置必须符合企业的内部控制制度，体现会计核算客观、及时、清晰的会计处理原则。例如，按照不相容职务分离的原则，出纳人员不得兼任稽核，会计档案保管，收入、支出、费用、债权债务账目登记的工作，所以，被授予出纳模块现金日记账、银行日记账等业务权限的操作员，就不应被授予凭证审核、凭证过账以及往来辅助账的对账与销账等项目权限。

（2）体现关联操作需要。得益于软件功能的拓展以及权限项目的细分，用户权限项目的组合灵活度非常高，其中一些权限项目针对同一操作而设置，而有些权限项目则共同关联一项完整业务的多个处理步骤。许多权限项目是相互关联的，其中一个项目权限的行使必须以另一项目权限的拥有为前提；或者，一个权限项目的执行必然导致另一项目也被同时执行。例如，审核记账凭证之前，必须先查询凭证，而编制会计报表或编制银行存款余额调节表之后，一定得输出这些表单等。所以，管理员对用户权限的设置必须考虑到操作项目的相互关系，将属于关联结果或必要前导的项目权限同时授予特定的操作员。软件本身也能判断某些权限项目的关联关系，当用户被授予某一操作权限时，其关联操作权限会被自动选中。

（3）岗位权责需匹配。在全面信息化的ERP工作环境下，各类人员的分工协作安排更加明确，岗位意识与权力意识大大增强。特定会计岗位的人员被赋予了必要的权限，从而可以凭借区别于他人的实际权力完成自己的工作，这种感觉能提升会计人员的使命感与满足感。在此，作为管理员，尤其要注意

会计岗位与会计人员职责的关系，既要使会计人员充分掌握完成所承担工作的必要权限，又要防止过度授权而导致的不必要的职权重叠。在权限配置过程中，宜根据权限的主次关系或重要程度来建立授权秩序，谨慎处置可能对企业业务造成影响或滋生舞弊行为的重要权限项目。

3. *权限控制策略*。为充分释放和利用权限管理中蕴含的能量，应在建立基本授权规则基础上采用适当的策略。

（1）建立用户权限管理制度。财务工作本身有不少的规章制度，不妨再增加一项“用户权限使用规则”，规范权限新增、修改、关闭等的原则与流程，强调权限应用规则与使用限制，同时要求操作员重视自己所拥有的权限，自觉维护权限与职责的严肃性。

（2）根据岗位与职责变动，及时调整用户权限。当会计人员岗位发生变动，或岗位职责有所调整时，要及时对用户的操作权限进行相应的调整。对于涉及职责变更的操作员，在追加其新增的职责权限的同时，应删去其原任岗位或职责中不宜保留的权限。通过合理的职权配置，提高用户权限的合理性与安全性。

（3）相互牵制，互相监督。利用会计业务内含的相互牵制关系，让不同岗位或不同作业环节人员的权限承载相互配合与制约的功能。出于保障软件及数据安全的需要，也可有意将某项业务所必须经历的不同步骤的处理权限授予不同的操作员，使会计人员通过协作与配合共同完成业务处理过程。笔者曾在用友ERP应用环境下设置销售出库单生单业务时，有意置空销售管理模块的“销售生成出库单”选项从而关闭了系统自动生单功能，使仓库人员在库存管理模块中必须调阅发货单或销售发票才能生成出库单，为仓库管理员添加了一个读取销售业务表单的步骤，从而为发现可能存在的业务错漏增设了一道防线。此外，某些分解与组合形式的权限配置，也有助于各岗位人员对企业会计工作整体的了解，有利于形成团队协作的工作氛围。

（4）发挥操作日志的检查监督职能。管理员可通过系统操作日志观察用户权限的使用情况，发现有违规使用操作权限或配置错漏时，应立即予以制止或调整。

三、密码控制规范及其对用户权限的影响

密码是开启权限之门的钥匙，也是阻挡非法侵入者的武器。建立密码机制是软件的必然要求，使用与管理密码也是用户的当然选择。

1. *密码与权限的对应关系*。会计信息系统的密码一方面明确了软件操作员所拥有的权限，另一方面也是对保护企业商业秘密实际举措的有力支撑，而这两方面都依赖于全体用户的共同遵守与常规维护。由于密码与权限是一一对应的，丢失密码意味丧失相应的操作权，从而暂时失去工作能力；而泄露密码则可能导致权限失控，会使企业内部信息面临泄露或被篡改的风险。所以，用户必须严格遵守密码使用规范，维护密码的严肃性，一旦密码被泄漏，就应立即采取相应的补救措施。

2. *密码设置中对用户权限的辅助管理*。系统管理员被赋予了用户权限管理的职责，而操作员密码的初始设置权则通常被绑定在用户权限管理工作之中。在用友ERP-U8系统中，系统管理员（默认admin）通过用户管理功能增加一个新用户时，可以为这一用户设置初始密码（口令），必要时还可通过修改用户信息的方式实现对用户密码的再设置。设置或重置密码的过程，事实上关联到对用户权限的设定或再配置，用户获得密码与失去密码的过程，也就是相应操作权限被授予和被剥夺的过程，必要时管理员还可通过密码效用开关直接终止或开启操作员的权限。

3. *密码丢失时的复权手段*。密码尽管重要，但丢失（或遗忘）密码也是常有的事。在ERP系统中，可以利用一般操作员、系统管理员、系统（技术）维护员之间所具有的不同管理职能体现在密码管理上的牵制关系，由享有较高专项处置权限的人员处理下一级别人员的密码问题。用友ERP-U8系统中管理员直接取消或修改一般用户的密码的做法，是一种比较直接、有效的密码重置方式。如果系统管理员的密码被遗忘或被非法重置，那么就需要求助于数据库系统维护员了。系统维护员既不能登录各项业务子系统，也不能以用户的方式打开系统管理窗口，但必要时可注册登录软件系统进入各相关数据库，直接修改或开启一般用户甚至系统管理员的密码与权限，达到重置密码或恢复权限的目的。但这类修改属于对软件应用环境有直接破坏可能的高风险操作，行使这一权限时必须要有第三方人员全程监督，并将恢复事项严格限定在目标用户原有的应用权限范围内。

四、权限控制中的应用创新与布设技巧

ERP系统涉及众多的应用领域与管理层次，其权限的有效配置，将在充分发挥各部门各岗位工作人员职能的前提下，有效保障系统数据的安全。

1. *智能进程域权限的布设与激活*。进程域权限是指被严格限定在某一业务处理过程的操作权限。这里的业务处理过程可以是时间段，也可以是业务环节；设置的权限可以绑定在某个业务进程中，也可以由特定操作事项来触发。这种权限有确定的应用目标，有明确的时间域或关联进程。进程域是指某一用户被授予的某一特定操作权限的作用范围，其基本数值取决于操作员岗位与业务的对应关系。

从技术角度来看，进程域权限设置功能可以由软件程序提供，也可以由管理员通过对基本权限的配置来实现。例如在用友软件中，可利用系统提供的项目权限与数据权限的双重配置来设定特定用户对于特定操作事项的处理权限，并通过账套主管对两项权限配置功能的效用控制予以激活或关闭。

在往来账项管理权限设置中，笔者曾将销售部用户的账项处理权限与往来款项金额范围进行关联设置，分别为销售专员、大区经理、部门经理、总经理设置了以10万元、20万元、50万元为界的警示触发限额，并设置了以30天、60天、90天为界的账龄警示期限。10万元以下小额业务或1个月以内短期账龄的账项由基层销售员直接管理，而50万元以上的大额业务或3个月以上较长账龄的高风险账项归集在上层业务负责人手中，同时将大额、长账龄业务的风险警示自动弹出频率由每7日一次提高为每3日一次。这使相应业务岗位的操作员具有与其职位相适应的往来款项处理的职责和权限，既释放了往来业务管理的能量，保证对一般往来款项进行催收、结算、调整等处理的权限需要，又满足了对大额客户（供应商）的重要往来事项的控制要求，从内在机制上维护了处理重要会计事项的谨慎性原则。

2. *内在互斥机制的建立与利用*。财务软件的功能或权限，会因会计业务的本质要求与控制需求而具有不相容的特征与要求，即互斥，其中包括不可为同一操作员同时拥有的功能互斥和不可授予同一操作员的权限互斥。

功能互斥是财务会计规范在软件中的功能体现，常见的单证录入与审核的分离、日记账与分类账的菜单分置等，都是对会计规范与内部控制要求的诠释；权限互斥则大多由系统管理员掌握，通常需通过权限配置来实现，如重要会计事项的多层级审核、账证表单的按类分管等，都可由管理员根据会计人员的职责划分予以设置。

在对某一流通企业基于用友ERP-U8系统的核算环境设置中，笔者曾利用应收应付款管理模块与总账模块对于往来科目使用许可的互斥关系，通过科目参数中“辅助核算”复选项与“受控系统”列表项的选择，将“应收账款”等往来科目的控制权定向到应收款管理等专项核算模块中，并关闭总账参数中的“可以使用应收应付控制科目”选项，从而开启总账凭证对往来科目直接应用方式的内置排斥功能，同时对专项模块中的往来账、账龄分析等进行适当定义。如此，应收应付业务处理权被限定在专项业务核算模块，使往来账项的记录、核销、输出以及账龄的分析与利用都在一个模块内完整地呈现，提高了往来业务的独立性及其后续管理的方便性。

3. *高风险功能的应用限制与动态授权*。ERP系统要求供应链等其他环节的人员参与会计核算工作，某些环节操作人员的会计专业水平或软件应用能力可能不能满足业务要求。为方便用户，通用软件往往提供突破财务会计规范的一些特殊应用功能，如反记账和反结账、跨期恢复、一条龙修改等。个别功能会使操作员的权限远远超过会计规范的约束范围，从而为信息错漏甚至会计舞弊打开了方便之门。

系统管理员有权力也有责任全面审视软件的功能，对可能导致账务错漏或秩序混乱的功能，应尽量缩小授权面，或者关闭其应用通道。同时，通过培训、辅导等方式提高操作员的专业水平，使这些可能导致会计数据发生本质性改变的高级功能被限制在最小的安全范围内。

在应用技术层面，可以采用权限开关或权限分置方式，为这些功能添加一个动态授权验证过程，即将功能权限授予业务处理的职能当事人，而将这一权限的激活权限授予另一个有审查判断能力的用户，或授予上一级业务负责人。当某一操作员需要利用这一功能时，则必须借助于另一操作人员的定向定时授权，如此可在最大程度上维护会计工作的严肃性，保证这些有操作失当风险的功能能够被正确利用。

主要参考文献：

黄辉，楼佳佳. 用友U8的权限设置细分[J]. 财会月刊，2013(7).

郑述招，周文琼，申艳丽，王二威. 金蝶K3中用户权限设置及其对业务的影响[J]. 财会月刊，2015(9).

作者单位：湖州职业技术学院商贸与经济管理学院，浙江湖州 313000