ERP 系统风险管理研究

文 勇

(广东科技学院财经系 广东东莞 523083)

【摘要】本文基于《企业内部控制基本规范》和《企业内部控制应用指引第 18 号——信息系统》,对 ERP 系统生命周期中的主要风险进行识别与分析,进而提出风险应对与风险控制策略,为企业提高 ERP 系统建设成功率、加快信息化进程、有效控制和规避风险提供参考。

【关键词】ERP 系统 风险管理 内部控制

ERP 系统集成了企业供应链上的物流、资金流、信息流等所有资源,为企业提供了系统化、全方位的信息化管理平台。然而,企业在 ERP 项目建设过程中并非一帆风顺,甚至不少企业以 ERP 项目建设失败告终,一个主要原因就是在 ERP 系统生命周期的每个阶段都存在着各类风险, 企业缺乏有效的风险管理措施。因此,企业必须依据全面风险管理思想,制定有效的 ERP 风险评估与控制策略,强化风险控制,将风险降低到可承受的范围之内。

ERP 系统目标设定是进行 ERP 系统风险识别与风险应对的前提,是企业资源计量的标准,不恰当的 ERP 系统目标会使企业承担不必要的风险, 或者因过于谨慎而耽误了企业的生产经营。ERP 系统目标可以分为战略目标和具体目标:战略目标阐明和界定了企业宗旨,是制定具体目标的依据:具体目标主要包括财务报告目标、经营目标、合规性目标三类。

风险识别与分析是根据风险产生的原因, 运用恰当的识别方法和工具找出影响预期目标实现的潜在隐患, 填制风险清单,进行风险分析和排序,明了风险形成的原因、过程和可能的结果,便于企业及时采取措施来控制风险。进行风险识别和分析后,企业应当综合运用规避、降低、分担、承受等风险应对策略,采取恰当的安全控制措施,将风险降低到企业可承受的程度。ERP 系统内部控制至少应该关注如下三大风险。

一、ERP 系统规划风险

信息系统规划可分为战略规划和执行规划。战略规划是根据企业发展战略目标,结合企业管理环境和信息技术,制定的信息化建设的长期性、全局性的宏观规划。执行规划是对战略规划的具体落实。

1. 信息系统战略规划的风险分析与控制。制定信息系统战略规划应当关注的风险:①缺乏全面综合的系统战略规划就仓促上马,使企业现有资源没有得到充分的开发利用,达不到预期的效果。②对系统实施的复杂性、艰巨性认识不足,仓促上马,贪大求全,要求 ERP 系统各模块一步到位,在准备不足的情况下盲目加大初期投资,致使管理跟不上,维护困难。③以为采用了知名软件公司的 ERP 系统就可以解决一切问题,从而忽视企业业务流程重组、企业管理层观念更新和员工业务素质的提高等其他关键成功因素。

这个阶段应采取的风险应对与控制措施:①充分考虑信息系统的目标、约束与总体架构以及企业资源和业务流程的现状,运用企业系统规划法、关键成功因素法或战略集合转移法制定信息系统战略。②成立系统规划领导小组,并对高管人员、分析人员和规划小组成员进行战略规划方法的培训,发挥业务部门和信息中心的积极性,加强各部门交流沟通,提出实施进度和步骤。③将业务流程重组的理论和方法与 ERP 系统相结合,对企业业务流程进行革命性再设计,使业务流程更高效、内部控制落到实处。

2. 信息系统执行规划的风险分析与控制。制定信息系统执行规划应当关注的风险是:①未根据企业战略要求、管理环境和资金实力来确定系统预算, 只做出系统购置或开发的预算,没有将系统实施咨询、培训、维护、二次开发等费用列入预算范围,使预算误差太大,不利于管理层对是否开发系统做出正确决策。②未合理划分信息系统开发阶段,各阶段任务不明确,导致项目进度滞后,质量难以保证。③为了“形象工程”或者迫于舆论压力,在未综合考察企业环境状况、信息化水平和资源的情况下,就开展 ERP 系统建设,使得项目达不到预期要求,无法满足企业的需求,以致半途而废。

这个阶段主要的风险应对与控制措施:①在系统预算方面不但要考虑开发或购买费用,还要为系统的管理咨询、售后服务留有充足的预算。②按照结构化系统开发方法、原型法、面向对象开发方法等,合理划分开发阶段,明确各阶段的任务和时间表,使项目按质按量完成。③由企业领导、系统分析师和信息管理专家组成可行性分析小组,对企业进行初步调查,从经济、技术、管理和法律上进行分析和评价,提出可行性分析结果,撰写可行性研究报告。

二、ERP 系统开发风险

ERP 系统建设有开发方式、外购与外包等方式,企业应根据管理需求、业务流程和信息化状况,做出合理选择,采取相应的风险控制措施。

1. 开发方式的风险分析与控制。系统开发有自行开发、委托开发、联合开发等方式。它们的基本处理流程相似,即分为系统分析、系统设计、系统实施等阶段。

(1)系统分析的风险分析与控制。系统分析是通过对现行系统的详细调查,描述业务活动与分析用户需求,从而提出新系统的逻辑模型,即新系统要"做什么"。这个阶段的主要风险是:①项目组需求调研不深入,对用户的业务需求理解不到位,造成需求未细化、描述不清,甚至出现需求遗漏和后续工作"南辕北辙"。②由于系统缺乏良好的整体架构,可扩展性差,难以适应企业变化发展的需求。

相应的风险应对与控制措施有:①加强系统分析师与业务人员的交流沟通。通过 UML 等标准建模语言和 Rational Rose 等建模工具,撰写需求详细、表达准确清晰的需求分析说明书。②构建灵活、高效、稳健的系统架构,使系统具有良好的可扩展性,为二次开发奠定基础。

(2)系统设计的风险分析与控制。系统设计是在系统分析得出的逻辑模型的基础上进行新系统的物理模型设计,主要解决"怎样做"的问题,它包括总体设计和详细设计。这个阶段的主要风险是:①系统设计没有遵循系统分析报告的要求,不能完全满足用户需求。②系统结构设计过于灵活,使系统实现和测试难度提高,系统的稳定性也受到影响。反之,系统结构设计灵活性较差,可扩展性较弱,就会增加系统维护的工作量和成本。③程序设计说明书和系统设计报告不健全、可读性差,导致系统实现、测试与维护阶段困难,甚至会造成灾难性后果。④没有将授权控制、用户管理、数据核算与检查、数据分析方法等内部控制措施嵌入系统设计方案,导致系统运行后衍生新的风险。

相应的风险应对与控制措施是:①系统设计人员应该与业务人员充分协商沟通,使系统设计方案能最大限度地满足用户需求。②系统既要有很强的稳定性和可维护性,又要有较好的开放性和结构的可变性。在系统设计中,尽量采用模块结构,构建"高内聚低耦合"的软件架构。③按照软件开发的国家标准和行业规范撰写程序设计说明书和系统设计报告,把系统设计人员个性风格限制到允许的范围,减少系统整合的风险。④在系统设计时要将生产管理业务流程、关键控制点和处理规则融入系统程序,实现手工内部控制的自动化。譬如:在财务管理系统中,输入的记账凭证借贷金额不平衡,或没有输入金额,或有借方科目而无贷方科目,或有贷方科目而无借方科目,系统应提示并拒绝保存。⑤应当考虑信息系统环境下新的控制风险,并设置相应的风险应对措施。例如许多软件操作不会留下审计线索,这就需要在系统中设置操作日志功能,自动记录何时何人登录系统并做了什么。

(3)系统实施的风险分析与控制。系统实施是将系统设计的成果付诸实现的过程。它的主要工作是:程序设计与编码、程序测试与系统调试、项目管理、人员培训、数据准备与录入、系统切换、运行、维护和评价。这个阶段的主要风险是:①程序实现的功能与系统设计相悖。②程序员对开发工具不熟悉,缺乏开发经验。不同程序员编程风格各异,程序可读性差,使系统难以维护。③测试人员经验不足,测试不充分,没能发现并纠正错误。④企业管理混乱,旧的规章制度和业务流程不完善;缺乏科学、统一的资源编码方案;粗放式经营管理方式导致基础数据的准确性、完整性和时效性较差,增加了基础数据采集的分析整理工作。⑤系统切换安排不周全,导致系统切换时影响到正常的生产经营运作。⑥初始设置时,相关账套参数设置仅能满足当前的业务需求,缺乏长远打算。

其风险应对与控制措施有:①建立程序代码审核制度,确保实现系统设计的功能和要求。②对程序员进行培训,统一编程规范,使标识与命名、注释等保持一致的风格。③明确系统测试的目的,成立专门的测试小组,精心设计测试用例,综合运用黑盒法、白盒法,对系统进行单元测试、子系统测试、系统测试、验收测试、回归测试等,提高用户参与度,尽可能组织独立的第三方专业机构进行验收测试。④根据企业信息化建设的整体目标,对企业现有业务流程进行颠覆性再设计,规范业务基础工作和会计基础工作,统一代码体系,整理录入初始数据。⑤制定并审核系统切换计划,包括人员培训、系统使用说明文档的编写、数据准备、实施步骤等内容。通过各种形式向企业全体员工灌输先进的管理思想、管理理念和管理方法。⑥系统初始化时,相关参数设置要有前瞻性和全局性,制定周详的数据迁移计划,并对迁移结果进行正确性测试。

2. 外购与业务外包方式的风险分析与控制。在外购调试、业务外包(如租用 ASP 或基于云计算的在线财务管理)方式下,企业很少参与系统设计和系统实践,可以适当简化风险控制措施,但在选择系统供应商、签订合同、跟踪评价等方面产生了新的风险,需采取相应的控制措施。

(1)外购调试的风险分析与控制。外购调试方式是指企业在软件市场上购买商品化软件,通过系统初始设置和二次开发建立本企业的信息系统。其优点是:软件产品成熟稳定;引入了先进的管理思想和方法;费用较低;开发周期短,即买即用;软件供应商有丰富的系统实施经验。其缺点是:系统实施费用较高,维护和扩展依赖于软件供应商。其面临的主要风险有:①选择的软件供应商缺乏可持续发展的实力,致使产品得不到及时升级更新,售后服务缺乏保障。②选择的产品在功能、性能、可靠性、可移植性方面不能很好满足企业需求。③在实施 ERP 或 MRPII 等大型管理信息系统时,没有聘请专业的咨询服务商,不少企业的业务无法与商品化软件有机整合,影响了软件功能的发挥。

其风险应对与控制措施:①广泛浏览相关网站和资料,听取专家的意见,以熟悉供应商、软件产品的特点;通过公开、公平、公正的招标方式选择供应商,确保中标的供应商有实力、讲信誉、售后服务好、产品升级能力强。②根据企业需求,合理选择产品的版本和模组。在确保软件成熟可靠的前提下,尽量选购业务流程和管理模式与本公司较相似的产品,减少系统实施的工作量。③出于成本方面的考虑,对于系统实施难度不大的中小型企业,可以选择软件供应商提供实施。对于业务复杂的大型企业而言,则需聘请行业经验丰富、对软件产品熟悉、深刻理解企业运作模式的咨询服务公司。在系统实施期

间,企业要注意培养自己的实施人才,以便将来业务发展和组织结构变化了,员工能实现系统的持续改进。

(2)业务外包的风险分析与控制。业务外包是企业委托专业软件公司或科研单位,按照本企业的业务需求进行信息系统的开发。其主要风险是:①委托代理关系使业务外包双方的信息不对称,承包方通常不能深入了解发包方的具体情况,而且很容易诱发偷工减料、疏忽懈怠,影响到整个系统的质量。而且,发包方对系统开发过程和开发技术不熟悉,更增添了项目的风险。②外包合同条款不完善、责任不明确,可能使发包方的合法权益受到侵害。③对外包项目跟踪评价不到位或者缺乏监测评价机制,使外包产品质量达不到企业要求。

其风险应对与控制措施:①通过严格的审批管控流程,利用公开招标的方式,参照业界基准,选出资质条件好、资金雄厚、信誉度高、服务态度好、有相同或相近承包服务成功案例的企业做承包商。②将标的技术的内容、形式、要求,开发计划,技术资料保密,开发计划与周期,开发经费及结算方式、验收的标准和方式,技术成果的归属和分享,风险的承担、违约金或损失赔偿的计算方法等问题在合同中详细说明,并由法律顾问审查把关。③引入IT审计制度,由独立于发、承包双方的"第三方"审计人员对软件的整个外包生命周期(包括软件发包、系统规划、系统分析、系统设计、系统实施、系统运行与维护、灾难恢复与业务持续计划)进行IT审计。同时,还可以引入监理机制,促进外包项目建设的规范化,降低风险,保证工程进度、质量和效益。

三、系统运行维护和安全管理风险

1. 日常运行管理的风险分析与控制。日常运行管理是系统切换完成并投运后的主要工作,主要工作内容包括系统的日常操作、系统运行情况的跟踪记录、系统运行的日常维护及系统的适应性维护等,主要目标是保证系统正常运行。这一环节的主要风险是:①缺乏科学规范的系统日常运行管理制度,可能导致系统隐患和故障。②缺乏例行检查,可能导致系统遭受自然、人为等因素破坏。③没有定期备份,一旦数据丢失或被人篡改,就无法恢复,影响系统的正常运行。④系统没有经过申请、审批、执行、测试环节就随意变更,变更后系统运行不稳定,达不到预期效果。⑤电子商务给企业带来了战略、系统、信息、市场等方面的新风险。

其风险应对与控制策略是:①建立系统操作管理制度、机房管理制度、文档管理制度,规范操作,保证信息系统的持续稳定运行。②对系统输入过程进行严格控制,保证数据输入与输出的结果正确。③设置系统操作日志功能,实时动态记录系统运行情况。④配备专业人员负责系统维护,应对突发事件发生,必要时应与系统研发公司或软硬件供应商会同解决。⑤系统日常维护主要包括:硬件维护主要做好设备的保养、故障检修、易损件更换与安装、设备功能扩展。软件维护是系统维护的主要内容,包括预防性维护、纠错性维护、适应性维护、完善性维护。数据库维护包括数据库安全性和正确性控制,数据库备份、重组、重构以及性能监控。⑥软件维护要遵照相应流程操作。⑦在对系统进行适应性维护时,应将访问授权控制、财产保护控制、数据转换控制、会计系统控制、内部报告控制、信息技术控制等的变更移植到企业管理运行环境中。⑧电子商务环境下,企业要加强电子商务的人才管理和培养,运用SWOT等方法进行分析,将战略风险降到最低。政府和社会要加强社会诚信和社会公德教育,完善企业的信用评价体系,建立健全法律法规,保证电子商务的正常运作。

2. 系统安全保密的风险分析与控制。这一环节的主要风险是:①道德风险。它主要来源于企业内部业务人员、关联方和社会不法分子有意或无意对系统的破坏。②系统故障风险。它是指硬件、软件、网络出现故障而使数据丢失、系统崩溃的风险。例如:自然灾害或意外事故引起的软硬件损坏和数据丢失;电子数据被拷贝却不留痕迹;剩磁和电磁辐射可能导致信息泄露;病毒干扰使软件和数据遭到破坏。

其风险应对与控制措施是:①设置信息管理部门,负责企业信息资源的规划、配置、协调、安全、管理等工作,信息主管向单位最高领导负责。②建立健全信息系统安全保密制度与泄密责任追究制度,对业务人员进行教育,提高其风险意识和风险应对能力。③建立信息系统相关资产的管理制度,硬件与网络设备未经授权,不得接触;设置存取控制,建立不同等级信息的授权使用制度,既要给合法用户提供必要的资源,又要防止非法的越权操作。④岗位设置和权限分配要遵循不相容职务分离控制原则。关键的业务系统,可以采用数字签名、数据加密、生物识别等技术方法识别用户身份。⑤利用软件系统、数据库系统、操作系统提供的安全功能,设置安全参数,确保系统访问安全,防止员工擅自装卸软件或改变系统配置。⑥综合利用杀毒软件、防火墙、入侵检测、漏洞扫描、隧道(VPN)等软件技术加强网络安全,严密防范病毒入侵和黑客攻击。⑦建立数据定期备份制度,规定备份时间、范围、方法、责任人、保存位置等内容。重要档案要做双备份,分别存放在不同地点,并做好防火、防潮、防磁和防尘工作。另外,在销毁关键数据和机密档案时,需按档案管理办法,经相关部门领导审核同意后,采用碎纸机等方式进行销毁。⑧定期对信息系统进行安全审计,发现系统风险及时加以控制,防患于未然。

ERP系统是企业的神经网络,对内部控制起着关键的作用,因此企业负责人应该将ERP系统建设作为一项重要工程来抓,整合企业资源,加大投入,制定科学规划,使信息系统建设有条不紊地进行,从而优化业务流程,降低企业风险,全面提高企业的经营管理水平。

主要参考文献

1. 蒋占华.企业内部控制配套指引讲解及案例精析.北京:中国商业出版社,2011

2. 袁广达. 基于环境会计信息视角下的企业环境风险评价与控制研究.会计研究,2010;4

3. 杜美杰.信息系统内部控制:过程控制和环境控制的结合——解读《企业内部控制应用指引第18号——信息系统》.财务与会计,2010;12

4. 李连跃.基于全生命周期的ERP风险管理研究.暨南大学硕士学位论文,2008