信息化环境下如何开展企业风险管理内部审计

杨 光

（浙江万里学院 宁波 315100）

【摘要】本文在简要介绍内部审计、风险管理与风险管理审计基本概念的基础上，分析了信息化环境下风险识别、风险评估和风险应对三个方面的审查与评价应重点考虑的因素，提出了信息化环境下开展风险管理审计的对策。

【关键词】内部审计 风险管理 信息化 风险管理审计

一、内部审计、风险管理与风险管理审计

内部审计是现代管理的组成部分。《内部审计实务标准》将其定义为：内部审计是一种独立、客观的保证工作和咨询活动，其目的在于为组织增加价值并提高组织的运营效率，采用系统化、现代化的方法对风险管理、控制和治理程序进行评价和改善，从而帮助组织实现目标。

美国反虚假财务报告委员会（COSO）在《企业风险管理框架》中对企业风险管理的定义如下：企业风险管理是一个过程，它由一个主体的董事会、管理当局和其他人员实施，应用于战略制定并贯穿于企业之中，旨在识别可能影响主体的潜在事项，管理风险以使其在该主体的风险容量之内，并为主体目标的实现提供合理保证。

内部审计在 COSO 这一框架中作为监控活动存在，由内部机构对企业风险管理进行独立评估。内部审计在企业风险管理框架中的首要角色是监督者，包括对风险管理流程的评估和保证服务，对风险评估准确性的保证服务，对关键风险报告的评估和对关键风险管理的评估。

二、风险识别的审查与评价应重点考虑的因素

1. 信息化环境下系统风险加大。在信息化环境下，以磁性介质等作为信息载体，存储在计算机磁盘上的数据容易被修改，甚至能不留痕迹。由于系统的分布式、开放性甚至远程处理的特点，数据的一致性保障更难，系统恢复处理的成本更高。系统风险不仅与内部人员道德风险有关，还广泛受系统关联方道德风险甚至社会道德风险的影响。

企业使用信息化业务流程，拥有高度集成的功能，并且系统用户无论在哪都可以访问系统，甚至控制或改变重要业务参数。信息化的这一特点虽能使企业员工以更大的灵活性去处理问题并提高效率，但如果对这种灵活性缺乏有效的控制，那么信息化的高度集成性和分布式的系统技术结构同样会为企业带来风险，信息化系统中高度集成的功能模块使得任何一点出现问题都会影响其他模块的正常运行。

2. 内部控制方式更为复杂。信息化环境下内部控制的方式发生了很大的改变，除了人这个执行控制的主体，还有许多控制方法通过软件来实现，因而内部控制也由单一人工控制转为人工控制和程序控制相结合的方式。授权控制是信息化环境下主要的组织控制原则，经办人员利用授权输入口令，获得相应的权利处理授权范围内的业务，保证系统的正常工作。要达到企业管理的目标，必须重视应用程序和操作程序。总之，信息化环境下内部控制也由人工变为人和计算机共同控制，导致内部控制方式更为复杂。

3. 数据的安全性降低。在信息化环境下，存储介质由纸张转变为磁性介质等，数据的共享程度大幅度提高，相应的，数据面临的风险随之增大。同时，由于信息来源渠道多样化，在原来单机系统中作为重点控制的输入控制就要扩展到所有数据收集和加工领域；由于数据传输的及时性，某个用户的一项数据错误可能在纠正之前已对其他用户产生了影响并进而形成了衍生错误。在这种情况下，数据的安全性必然降低。

4. 内部控制制度有可能弱化。在信息化环境下，出现从事数据输入输出的人员随意修改数据的情况，会加大系统的风险。主要有以下几种表现：

（1）职责分离原则执行不彻底。一些企业的程序员或系统的维护人员往往随意接触系统，甚至顶班操作，也有一部分企业常有同一人用不同的密码去完成数据输入与复核两项不兼容的工作，使应有的控制完全失效。

（2）系统的恢复控制薄弱。虽然大部分企业的数据文件都有备份，但对备份文件的保管并不完善，很多企业基本没有制定系统遇到毁损时的恢复计划。

（3）内部审计监督弱化。由于我国的内部审计制度不够完善，内部审计人员素质普遍不高，一般不熟悉信息化环境下企业的特点和风险，不了解信息化环境下应有的内部控制，更不熟悉信息化环境下如何开展风险管理审计。因此，高风险的信息化环境系统未能得到有效的内部审计监督。

5. 系统资源多样化增加了管理的难度。由于信息化环境下系统的牵涉面很广，信息化环境下的软件、硬件、数据资源十分丰富，各自的内容和标准多种多样，对系统的检查难度加大，对系统管理的难度也随之增大。

6. 内部控制内容复杂化增加了控制的难度。信息化环境下数据的使用面扩展到整个网络，这就使得内部控制要关注

的对象不仅仅是会计系统，而且要向业务管理信息系统及其供应链追溯；不仅仅局限于内部，而且还包括外部控制。信息化环境下出现了许多新的控制特点：网络规模不同，外部控制的范围也有很大的差别，当企业内联网成为互联网的组成部分时，外部控制就包括了周界控制、大众访问控制、电子商务控制、远程处理控制等，使得内部控制的难度增大。

7. 无纸化交易加大了管理风险。在信息化环境下纸质记录减少了，取而代之的是存有数据处理资料的磁盘、光盘、移动硬盘等磁性介质。这些介质的数据处理都由计算机自动完成，因而产生了大量的无纸化交易，致使很难通过纸质文件直观跟踪业务的处理过程，也无法用传统的方法考查业务的安全性、完整性和准确性，从而加大了管理的风险。

三、风险评估方法的审查与评价应重点考虑的因素

1. 信息化环境下系统风险加大的可能性和影响程度。内部审计人员要对信息化环境下系统风险加大的可能性和影响程度进行审查与评价。在信息化环境下，内部控制依赖于人和软件，由于内部控制融于系统软件之中，审计人员无法通过传统方法察觉，对系统设计中存在的缺陷也难以发现。如设计计算机信息系统时考虑不周，缺乏应用软件的控制能力，系统可能无法判断某类数据是否符合逻辑，对不合理的数据可能也会进行日常处理。并且对错误数据的处理还具有重复性和连续性，从而可能导致整个系统出现错误的数据，系统风险加大。

2. 内部控制方式更为复杂的可能性和影响程度。内部审计人员要对内部控制方式更为复杂的可能性和影响程度进行审查与评价。信息化环境下存在实时控制失控的可能性，有些数据难以实时同步，而且存在双方数据不一致的可能。

3. 数据安全性降低的可能性和影响程度。内部审计人员要对数据安全性降低的可能性和影响程度进行审查和评价。信息化环境下存在电子数据被滥用、篡改和丢失的可能性。在信息化环境下，由于存储介质的改变，信息高度集中于计算机信息系统，信息系统应用程序被恶意篡改，或非法入侵信息系统造成经济损失的可能性致使审计的固有风险增大。一旦用户非法穿过计算机系统的“防火墙”，数据被不法分子拷贝，甚至篡改而不留任何痕迹。计算机病毒、电源故障、操作失误、程序处理错误和网络传输故障也极易破坏和修改电子数据，造成电子数据与实际数据不相符，数据的安全性降低。

4. 内部控制制度被弱化的可能性和影响程度。内部审计人员要对内部控制制度被弱化的可能性和影响程度进行审查与评价。在信息化环境下，一是通过划分操作员的责任范围，设置权限和密码实现人员职责分工，二是通过软件设计划分若干子系统或功能模块，设置不同的责任中心。由于在计算机信息系统中许多不相容职责相对集中，可能因为不恰当的授权而使内部控制措施有可能形同虚设。

5. 系统资源多样化增加企业风险的可能性和影响程度。内部审计人员要对系统资源多样化增加企业风险的可能性和影响程度进行审查与评价。在信息化环境下，信息技术控制包括数据存储控制和数据处理控制等，系统资源多样化增加风险的审查与评价，如对程序变化的检查能否确保系统程序按管理当局的意图运行；在网络灾难导致数据存储平台或数据处理平台瘫痪时，灾难防御计划能否使信息处理功能迅速恢复，这些可能性和影响程度都是需要加以关注的。

6. 内部控制内容的复杂化增加企业风险的可能性和影响程度。内部审计人员要对重点的内部控制内容增加风险的可能性和影响程度进行审查与评价。

7. 无纸化交易增加企业风险的可能性和影响程度。内部审计人员要对无纸化交易增加企业风险进行审查与评价。无纸化存在审计线索被减少或消除的可能性，在信息化环境中，从原始数据录入到报表的自动生成，传统的审计线索不复存在，给审计人员查找审计线索带来了较大困难，审计人员应该特别加以关注。

四、风险应对的审查与评价应重点考虑的因素

1. 并发控制是否适当和有效。由于在信息化环境下各工作站都可能随时访问服务器上的共享数据，这就有可能存在两个或两个以上的用户同时对同一数据进行操作，如果对这一在单机系统中不可能存在的冲突问题不加以控制，必然会造成整个系统数据的混乱。所以审计人员应了解并测试系统在处理两个或两个以上的用户对同一数据的操作发生冲突时所采取的应对措施是否适当和有效。

2. 信息安全控制是否适当和有效。信息化环境下的分布式操作使得对系统的攻击可以从多个方面进行，而对于企业内部使用者来说，如果保密制度不当、内部控制不严，也容易造成信息的滥用和外流。通讯线路可能存在的窃听、通讯传输中的线路干扰和噪声都直接对信息保密性和完整性造成破坏。审计时应审阅控制台和控制工作站对系统使用情况的详细记录，了解有关通讯控制和权限控制的内容和技术、网络中数据加密和端口保护措施，并做出评价。

3. 数据库的自动验证措施是否适当和有效。在信息化环境下通常采用诸如 ORACLE、SQL SEVRER 等大型数据库以解决小型数据库无法完成的海量数据处理、高速运行和数据安全问题，但数据差错仍不可避免。数据的一致性、可匹配性在信息化环境下尤其突出，应建立相应的自动验证系统，审计人员应通过对数据库具体内容的检查、余额平衡检查、数据合理性检查来验证数据库的自动验证措施是否适当和有效。

4. 系统的恢复控制是否适当和有效。在信息化环境下系统运行过程中可能出现许多在单机系统中不会出现的问题，意外峰值数据超过通讯软件的承受能力、外围设备发生故障、代码不一致造成的数据混乱、黑客和病毒攻击等问题可能随时出现，导致系统不能正常工作，甚至黑客从中窃取数据。审计人员应检查系统的处理、备份（包括硬件和数据）和断点恢复及校验措施，在出现意外情况时能使系统迅速恢复运行等应对措施是否适当和有效。

5. 不相容职务进一步集中化的补救措施是否适当和有效。由于在信息化环境下系统的规模更大、自动化程度更高，原来的不相容职务（授权、执行、记录、资产保管等）可能进一步向信息管理部门集中。例如，系统设定了某种存货安全存量标准，当该存货库存量低于该标准时，系统可能自动从网上向

关系客户发出订单(内部系统也有可能自动根据某项设定自动向其他部门如仓库发出调拨通知),这就造成授权、执行、记录职务集中于信息管理部门。审计人员必须检查系统是否采取了必要的补救措施来消除因不相容职务的集中化而导致的错弊,发现问题并提出改进建议。

五、开展风险管理审计应采取的对策

1. 健全信息化环境下相关内部审计准则。内部审计工作中已建立了一系列的审计准则。但是,由于审计线索、审计内容以及审计技术手段等发生了一系列的变化,手工审计中所制定的审计准则也就很难在信息化环境下适用。在信息化环境中可能出现新情况并产生新问题,但与之相适应的新的审计准则还有待制定。可以借鉴国际审计准则和中国注册会计师审计准则,如美国执业会计师协会 1984 年发布的《计算机处理对检查财务报表的影响》,国际会计师联合会 1984 年公布的《国际审计准则 15——电子数据处理环境下的审计》、《国际审计准则 16——计算机辅助审计技术》等来健全我国的内部审计准则。

2. 发挥内部审计的优势,积极推进风险管理审计。内部审计不参与企业生产经营业务的具体管理,也不对各项业务管理中的问题承担直接责任;内部审计涉及的范围覆盖企业的各个方面,掌握的信息是多方面的,有从全局考虑分析判断风险的综合性优势;内部审计部门和内部审计人员长期在企业内部工作,对企业面临的风险更了解,对风险的各种影响因素更便于进行深入的调查,有能够连续参与风险管理的优势;内部审计人员作为企业员工,由于最终利益的相关性,也会对企业风险管理的效果和建立风险管理的长效机制更有责任感(侯瑞霞,2007)。风险管理审计是企业内部审计人员通过测试风险管理的有关方面(风险管理方针、策略和风险评价指标体系),对风险程度及管理情况作出专业判断,提出审计评价和建议,以实现企业运营目标。其根本目标是通过将风险与企业目标的实现直接联系起来,为公司治理层及管理当局提供有价值的服务。目前我国风险导向内部审计尚处于起步阶段,亟待积极推进。

3. 将系统的安全可靠性作为审计的第一目标。在信息化环境下,系统的安全可靠性异常突出,所以只有在系统安全可靠的前提下才能考虑其他审计目标的实现。系统的可靠性除决定于系统的功能外,还决定于操作和内部控制,在信息化条件下,企业的内部控制包括程序化的控制和要求员工执行的管理制度,所以除对通过计算机软硬件实施的控制进行有效性评价外,还应对企业管理制度的完善性、适当性和有效性进行审计,在信息化环境下系统内部控制的符合性测试比单机条件尤其是手工条件下重要得多。

4. 充分利用信息化环境,不断更新风险管理审计的方法和内容。内部审计人员要充分利用系统的数据分析工具,充分利用系统数据集成的优势。信息化系统的实施在很大程度上改变了企业的业务流程,如 ERP 系统实现了从采购到付款、从订单的获取到发票的开出等业务集成,实现了跨职能部门的业务处理,因此,审计人员不需要再从多个系统获取数据,而仅由一个系统就能得到所需要的数据。审计人员要充分利用信息化提供的方便开展风险管理审计。如 ERP 系统本身提供了很多标准报表及报表编辑、分析工具,审计人员可以直接利用系统标准报表及报表分析工具,进行数据查询和分析。

信息化环境是一个管理信息系统,而管理观念和管理模式的发展变化很快,且信息化环境重视提供管理问题的解决方案而不是单纯的软件,如企业资源计划(ERP)和业务流程重组(BPR)就是基于信息技术为基础的新的管理思想。这些管理观念还在不断地发展更新,同时连接到网络上的子系统也一直处于动态的更新过程中,所以审计人员不能沿袭以前的审计模式,而要根据不同的系统及其最新的变化对审计的内容、方法、步骤进行重新设计。

5. 开展后续审计。由于种种原因,被审计单位有可能表面上认可审计结果,却没有采取任何实质性的改进措施,这不仅无法进行有效的企业风险管理,而且会动摇内部审计在企业中的威信和企业风险管理审计的存在价值。所以,后续审计就成了内部审计工作中的关键程序。后续审计应该跟踪如下问题:对于重大的审计发现,相关部门和环节是否予以纠正;若未予纠正,责任和原因到底在哪儿等。为便于企业高层理解审计部门的工作,保证审计建议的有效落实,后续审计也必须有具体、详细的跟踪记录。

6. 建立学习型内部审计机构,提高内部审计人员的风险管理水平。前已述及,在信息化环境下,由于经营环境日趋复杂,企业风险管理审计也日趋复杂,这无疑对内部审计人员提出了更高的要求。审计人员面临着更新知识的需要,他们不仅要有丰富的会计、财务、审计知识和技能,而且应掌握一定的计算机知识及其应用技术,还要掌握一定的现代信息处理和管理技术;从长远的观点看,审计人员还应当掌握相关审计软件的使用本领,建立自己的电算化审计系统。

为此,要建立学习型内部审计机构,营造整个内部审计组织的学习氛围,不但要学习书本知识,而且要从工作中学习,从项目中学习,积累经验,充分发挥内部审计人员置身于单位内部,情况熟、信息灵、便于从事经常性审计工作的优势。从而建立起一种能持续发展的内部审计组织,提高内部审计人员的风险管理水平。

7. 聘请专家共同参与风险管理审计。风险管理审计工作所面临的信息系统非常复杂,要搞好风险管理审计必须精通企业相关行业、产品、技术等方面的专业技术,对于大中型企业的信息化系统,几乎没有内部审计人员能够全面认识和理解整个系统的功能和每个模块的特点,这对内部审计而言是非常困难的事。我们要充分利用各类专家的专业技能推进审计工作,进行准确的审计判断。

主要参考文献

1. 程安林.信息系统环境下审计风险的特征及评估.北方经贸,2007;5

2. 孙清娟.内部审计参与企业风险管理浅探.湖北经济学院学报(人文社会科学版),2007;1

3. 王光远.现代内部审计十大理念.审计研究,2007;2