IT 风险及控制的应对与合规工作探究

●周元元 庄明来

摘要：随着计算机和现代信息技术在会计中的广泛应用，会计系统处理结果的正确性更多地依赖于内部控制制度的完善。信息环境对会计信息系统的内部控制要求更加严格，控制的范围也更为广泛。为了确保信息环境下会计内部控制的有效实施，文章从 IT 的视角对传统的控制观点进行改革，探讨了遵守“萨班斯—奥克斯利”法案时的整体 IT 风险的控制方法及应重点考虑的问题，并着重分析了 404 条款合规小组如何就 IT 流程层面的 IT 基础设施控制（ITGC）进行审核。

关键词：内部控制；信息环境；SOX-404；ITGC；ITAC

信息技术和网络技术的飞速发展和广泛运用对传统会计和审计来说不啻于一场革命，它改变了会计控制的性质，改变了会计信息存放、传输及加工处理的技术基础。随着会计信息系统在企业中发展的日趋成熟，控制环境发生变化，内部控制也呈现出新的特征。

一、从 IT 的视角更新控制观点

尽管会计首先大量使用计算机，使会计处理自动化，但会计师们在开发 IT 的应用能力方面却落在了后面。会计师和审计师的控制观点没有考虑 IT 对业务运行、对规则的符合程度和信息过程相关的风险的影响，并已经对帮助企业识别和控制业务过程的风险感到力不从心。因此，我们需要建立起一种新的控制观念，让 IT 有效地集成到业务和信息过程中，把保护企业和促进企业有机结合起来。

1. 扩大控制的范围强调第三方监督。传统上会计师和审计师常常采用标准驱动的观点，这在独立外部审计中更为明显。大部分审计活动和审计标准主要在年末检查财务错误和舞弊。审计师对财务报表的公允性及其是否符合会计原则进行检查时，只关注发表审计意见所必要的控制。但事实上，大部分针对业务操作和规章遵守情况的控制与财务报表的独立审计并没有关系。因此，在建立内部控制制度时，会计师们应该打破这种独立的、反映的和检查性的模式，以一种复杂的、积极的业务观点来帮助设计和实现业务的规则，在更广泛的环境中来看待业务，强调预防、业务操作和对规章的遵守情况。COBIT 模型对企业实践具有重要指导意义，它增强了 IT 控制在企业日常运营过程中的可操作性。此外，企业的控制漏洞依然存在，上市公司财务丑闻始终不断，原因究竟何在？本文作者认为，独立第三方监督的缺失是企业内部控制屡屡失败的根源。企业 IT 控制的有效实施同样需要一个统一的衡量标准，且该标准的制定方必须保持中立。显然作为 IT 控制的实施者和受益者——企业以及企业 IT 控制的重要参与者——会计师事务所等都不应该成为标准的制定方。事实表明，完全独立于企业经济利益的国家政府及其相关部门是执行企业内部控制（包括 IT 控制）监督职能的最佳人选，在这方面可以借鉴由美国政府出台 SOX 法案，其中 SOX-404、SOX-302 法案的苛刻内控要求隐含了对企业 IT 控制的控制要求。其制定的 SOX-404 影响深远而广泛，是衡量企业 IT 控制是否有效的事实标准。IT 控制是企业管理信息化下内部控制的新构成，SOX-404 在对企业内部控制提出要求的同时，必然对其 IT 控制做出相应的要求，且企业有效的 IT 控制是其内部控制体系的整体有效实施并通过 SOX-404 测试的前提。基于 IT 控制和企业整体内部控制的关系，针对 SOX-404 的控制需求，作者认为要实效的 IT 控制，就要首先理解公司的总体 SOX 合规计划，然后制定一项有关 IT 控制的计划，并做到 IT 控制计划与公司总体 SOX 合规计划的合理集成。

2. 特定控制程序分析。通常情况下，职责分离是传统内部控制的一个重要组成部分。职责分离——传统上，控制程序将下列责任分派给不同的人，将活动划分为一定的结构：(1)交易授权；(2)在会计记录中记录交易；(3)维护和保管资产。实施这种程序是为了防止雇员在正常工作中

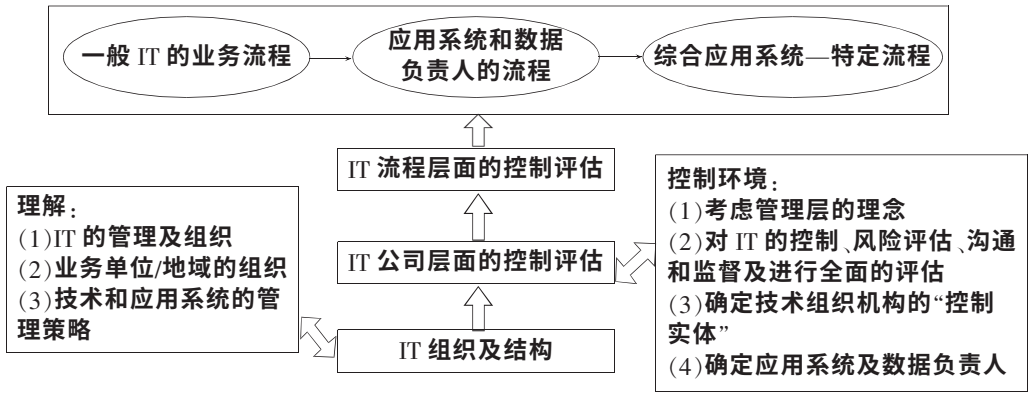

图 1 IT 风险及控制评估整体方法

发生错误和舞弊并将其隐藏。在手工环境下,分离这些职责(保管、记录和授权)是非常有用的。但 IT 应用的介入使有些情形发生了改变。如,传统的职责分离概念是让执行业务事件的人记录所有的相关的业务事件数据。而现在很可能几个部门同时由一个人在执行业务事件时实时地记录一个业务事件数据。自动控制处理代替了分离的人的角色,消除了一个人执行两项不相容活动的风险。在 IT 环境下,信息技术取代了人的作用,其监控能力更强。职责分离仍然是形成内部控制观点的重要概念。但它的适用方式发生了变化。这时,我们需要分离新的职责(保管、授权、操纵数据和信息),以反映用来设计和运行系统的手段的更新。

3. 强调预防。一般来说,内部控制制度是预防、检测和纠正风险的程序的集合。由于审计本身的性质,审计师一般主要关注检查性控制。审计的主要目的是对前一段时间的财务报表的公允性发表意见。而审计的这种思想也影响了会计。许多会计系统并没有与业务过程的执行相结合。因此,当数据最后到达会计系统时,及时预防甚至检查错误的时机已经错过了。一个有效的内部控制制度需要预防性的、检查性的和纠正性的控制。一旦检查出错误和舞弊,应该纠正其影响,同时制定预防性控制措施以确保错误和舞弊不再发生。如果能事先预防错误和舞弊,而不是事后检查或纠正,这样的内部控制将给企业带来更大的价值。

4. 选择设计和实施控制的时机。IT 在企业中的应用通过以下两方面提供价值:

(1)帮助企业更积极地预防、检查和纠正错误和舞弊。

(2)促进而不是阻止业务过程和信息过程的持续改善

要得到这些益处,必须具备"实时"的控制思想。控制应该嵌入到系统中,在每项业务活动中预防、检查和纠正,而不是在系统实现后再加入控制程序。正如 COSO 所认为的:"内部控制不应被看作是添加在组织正常运行结构之上的东西。这样做将削弱组织的竞争能力。内部控制应该被嵌入到企业的基础结构中。当控制与运行活动融为一体时,控制的观点将深入人心,组织将以最小的代价获得更好的控制……"。

因此,会计师和审计师在研制新系统或修改原有系统时,应在系统的设计和开发阶段积极介入,帮助提出控制方案和实施有效控制。

二、遵守萨班斯法案时的整体 IT 风险及控制方法

业务流程对技术的依赖程度逐年增加,使得业务的执行更加及时、全面及准确。财务报告流程及其他流程,即财务报告所记载的交易的获取、记录、汇总、计量及列报均需要依靠计算机程序即其他技术性的工具和软件来完成。因此,应用系统和系统的控制成效直接影响流程的完整性,包括输入流程的数据和流程完成时最终呈报的信息(即输出资料)。应用系统已有自己的控制程序。在这些程序化的控制中,有些可能是财务报告内部控制的关键,若这些程序化的控制起关键作用,在进行评估时就必须予以考虑,特别是在流程结果没有经过验证或者验证不足的情况下,管理层仍然需要依赖这些控制。IT 风险只在 IT 环境中存在,因此,由 IT 技术衍生的相关风险必须在评估与财务报告相关的内控风险时予以考虑。简而言之,在当今高度信息化的商业环境下,根据 Sarbanes-Oxley 第 404 条款的规定在进行财务报告内部控制的整体评估时,必须考虑有关 IT 的风险和控制。

404 条款合规小组应该如何定义 "IT 风险及控制"?404 条款合规小组应考虑的风险及控制包括 i)因技术(例如应用系统中的程序化控制) 而存在的风险及控制,ii)影响相关程序或数据完整性的风险及控制。此外,就 404 条款合规工作而应予以考虑的 IT 风险及控制, 只限于那些与实现财务报告可靠性该内部控制目标有关的风险及控制。因此,"IT 风险及控制"主要涉及两个大的领域-基础设施控制(ITGC)和应用系统控制(ITAC)。ITGC 通常会影响到技术环境内众多单一的应用系统及信息生成。一般来说,由于这些控制会影响相关程序和数据的可靠性,所以最终会影响财务报表认定的实现,即控制能防范或预防某些影响相关程序和数据可靠性的事件发生。ITAC 领域涉及一下两个重要领域:(1) 由相关的应用系统和数据负责人设计并实施业务中的控制及流程;(2) 应用系统中的程序化控制,负责执行控制有关的特定活动,例如在输入过程中对主要栏目中的被输入数据进行错误检查或验证。其中一个应用系统的控制的例子是不兼容职责的分离,数据负责人需负责设计及合理地判断哪些责任和职责被分离。程序编制小组在负责设计和开发应用系统,使交易能够按照系统负责人的设计旨意在程序化的和其他形式的控制下完成,为达到财务报告认定提供一定保障。

在进行财务报告内部控制的评估时,应谨慎考虑信息技术所产生的影响,包括一些 IT 所独有的风险。本文系统性的描述了 IT 风险及控制评估时所遵循的整体方法及有关框架。

图 1 说明 IT 风险与控制评估所应该遵循的顺序,每一个步骤都会影响范围的界定,有时候还会影响到下一步要进行的工作的性质。第一步是理解"IT 组织和结构",这一步为 IT 公司层面的控制评估奠定了基础。公司层面的控制的强弱又会影响对 IT 业务流程从三个层面进行控制评估的性质和程度。对 IT 流程层面控制的评估是 SOX-404 条款合规项目中最繁琐的一项工作。对 IT 流程层面的评估要从"一般 IT 的业务流程"、"应用系统和数据负责人的流程"以及"综合应用系统—特定流程"三个不同层面予以考虑。

1. 一般 IT 的业务流程。IT 基础设施控制的审核是针对公司的主要 IT 流程, 或是支持财务报告的关键 IT 应用系统。404 条款合规项目小组可能需要对同一个基础设施控制进行不止一次的审核,例如,多个流程同时影响每个重要财务报告领域, 而该流程又不是受限于相似的政策、流程活动和控制程序,那么该流程可能需要被分别予以审核。在评估一般 IT 流程中应该包括的基本部分: 安全管理、应用系统/系统变更管理、数据管理与灾难恢复、数据

中心的操作及问题管理、资产管理。

2. 应用系统和数据负责人流程。这方面被评估的是那些直接被应用系统和数据负责人控制和管理的程序。404 合规项目阶段应该予以评估的流程包括:建立和维持不兼容职责的分离(安全角色和管理)、确认/审核对关键交易和数据的存取、开发和维护业务影响分析/业务持续计划、制定和维护业务负责人变更控制。

3. 综合应用系统——特定流程。对业务流程层面的所有 IT 控制和人工控制进行综合评估是必须的。评估中有关 IT 的部分主要集中在对关键应用系统的控制,在对企业业务流程进行评估时也应该评估相关的 IT 风险和控制,从而对控制环境有全面了解。负责人应该对每个重要业务流程中关键财务应用系统的控制有充分的了解包括:应用系统程序化控制、关键交易和数据信息的获取控制、数据验证/错误检查程序、错误报告、复杂运算、报告的可靠性和准确性、关键接口。

三、SOX-404 条款合规小组对于 IT 基础设施控制的关注

"IT 基础设施控制"的性质对于财务报告内部控制评估具有十分重要的意义,但其产生的影响却经常被误解。本文作者认为 SOX-404 条款合规小组应该从流程的角度去了解这些控制。本文将 IT 基础设施控制细分为若干基本流程,阐述这些基本流程与财务报告的相关性。这些控制包括安全管理、应用系统的变更控制管理、数据管理和灾难恢复、数据中心操作和问题管理,以及资产管理与有关的流程。

1. SOX-404 条款合规项目小组对安全管理评估时的关注。在安全管理领域中,首要的流程目标是创建和维护 IT 环境的整体计算机安全措施。安全管理的焦点是全面性的,其中包括关于应用系统、数据库、平台、和网络的流程;还有其他的流程,涉及识别风险、制定策略以便将风险减低至可接受的程度,以及管理层明确接受剩余的风险或风险容忍度。安全管理需要一套有效的流程,一便执行及监控 IT 环境各个层面中的政策和流程的执行。此外,还有一些子流程,负责处理个别信息资产的存取,以及控制非授权存取的风险。在很多公司,安全管理是一个复杂且分散的流程,涉及众多的"技术层",分别由不同的 IT 部门负责处理。应用系统上的安全管理会被派发到不同的 IT 和用户群组。进行内部控制评估时的一个严峻的挑战是要了解公司是如何部署安全管理的。因此,404 条款合规小组须了解关于 IT 组织的足够细节,从而能够了解公司的关键数据及应用系统的授权获取及应用是在哪个"技术层"被怎样管理的。安全管理流程也包括如何管理那些拥有全面权限可自由访问系统中储存的各种交易及数据的特殊用户。公司应了解这些特殊用户的特殊权限存在的必要性(而且在需要情况下这些权限不能全部被限制);但是公司应具备严格的控制来尽量限制和监控这些特殊权限的使用。以下简要列出公司财务报告认定的影响,以及如何影响萨班斯法案 404 条款合规项目的范围:

安全管理流程对财务报告认定的影响:

(1)按业务需要限制对关键系统(交易、应用系统、数据库、平台和网络)的操作,以确保数据(资产)的访问权限。

(2)执行、审批和检视交易的权利只限于有正当业务需求的人士,以确保授权是按照管理准则适当受到限制。

2. SOX-404 条款合规项目小组对应用系统的变更控制评估时的关注。应用系统变更控制是财务报告内部控制中的一个尤其重要的因素。应用系统变更的可靠性会直接影响交易流程的准确性、一致性和完整性,以及交易的及时累积、总结和呈报。公司变更其应用系统时所面临的风险是:新的变更可能导致曾用于处理和呈报交易的应用系统,失去其原有的可靠性。这将造成财务报告不准确、不完整或不正确等潜在的重大风险。鉴于可能出现这些与财务报告有关的风险(以及其他显著的策略及业务操作风险问题),公司必须有一个涉及周详且运作有效的应用系统变更管理流程。该变更流程应包括适当的程序,以建立监督、测试及审批有关变更,并将经适当审批的变更转移至生产环境。该流程必须设置适当的保安措施,以防止负责该流程的人员在未被发现的情况下,对程序或有关数据做不适当变更。考虑到变更可能产生的所有影响,例如系统接口、数据和例行错误侦测程序、应用系统的安全管理变更、管理报告等,因此变更流程必须包括周全的措施及步骤。

应用系统的变更流程对财务报告认定的影响主要包括如下几点:

(1)应用系统的变更直接影响应用的安全性、准确性和一致性,这里的应用系统是指进行交易、将会计信息汇总、分类、计量和披露是所用到的程序。

(2)因为增加或修改职责或因为对敏感交易及数据的存取授权交易修改而作出对应用系统的变更时,可能影响不兼容职责的适当分离。

(3)在变更的操作过程中可能会使未获授权人士也能够存取信息资产,而这将导致应用系统或数据在无从被一般控制活动发现的情况下,被有意或无意地篡改。

3. SOX-404 条款合规项目小组对数据管理和灾难恢复评估时的关注。数据管理对技术组织的工作成效和效率起关键作用,为了便于讨论,我们将"数据管理"归纳为与数据备份、恢复和修复有关的流程。在很多情况下,需要进行数据的恢复大部分原因是由于硬件或者软件损坏而导致数据受损或遗失。公司必须有能力修复或重新启动系统,以确保持续操作及不损害交易或数据的可靠性和完整性。数据管理也包括应用系统的关键性,以及备份流程的合适时间和次数的考虑。备份流程的次数和可靠性反映出一家公司对成本/风险/收益的判断结果,即在不会对业务造成负面影响的情况下,该公司可以承受多大的数据损失或多少交易的损失。

灾难恢复的流程和程序是与数据管理相关联的。业务的持续运作和 IT 的灾难恢复,主要涉及公司是否能够持续遵照 SEC 的规则和条例、准确且适时的提交其财务报告

和其他报告。

数据管理和灾难恢复流程对财务报告认定的影响:(1)公司能否完整及准确的报告交易和财务报告数据的能力会收到数据管理和灾难恢复流程的影响。(2)如果透过数据管理流程而赋予对生产或备份数据不恰当的存取权利,资产的获取可能会受到影响。(3)如果业务持续运作和灾难恢复计划不够全面和得到及时更新,那么公司履行其义务的能力,即完整且准确的报告及时提交 SEC 的能力将会受到影响。

4. SOX-404 条款合规项目小组对数据中心操作和问题管理评估时的关注。数据中心的操作和问题管理也会像前面讨论的数据管理流程一样影响应用系统和数据。这些流程会影响数据的可靠性及程序的完整性和准确性。当有问题发生时,数据中心的操作和问题管理会影响应用系统的正常操作。在诸如接口的处理不完整或程序被中断等类似情况下,交易或数据的处理不完整不准确的风险概率就会增高。计算机操作和问题管理方面的步骤,旨在提供处理这些问题的方法。这些流程通常涉及数据和应用系统负责人之间就解决相关事宜和问题而进行的交流和沟通。此外,这些部门的负责人员通常在数据的存取和应用系统的操作方面拥有广泛的权力,以及时解决出现的有关问题。这就增加了交易及数据在非常情况下,未经正常授权下被存取的风险。

数据中心操作和问题管理流程对财务报告认定的影响:(1)报告的完整性、准确性和一致性会直接受计算机操作和问题管理流程影响。(2)如果没有适应的限制和监督计算机操作和问题的管理,信息资产的存取会受直接影响。

5. SOX-404 条款合规项目小组对资产管理评估时的关注。资产管理领域是现今 IT 组织中重要的一环。原因是除了硬件和软件价格不菲之外,在以往的管理过程中一直表现欠佳。从 SOX-404 条款合规项目的角度来看,资产管理的重要方面与 IT 资产的获取、操作和报废的正确会计处理有关。此外,该领域也涉及一些软件版权的适当使用及监督的潜在问题。不正确使用软件可导致未记录的负债以及围绕正确使用软件和遵守软件使用法例而产生的潜在信息披露问题。就公开报告的角度而言,另一个值得关注的领域是对资产存在的定期验证、记录余额的定期评估以及根据使用年期进行的资产变现。有关 IT 资产管理的主要报告问题,与有关所有固定只产的报告问题并无差异。该 IT 资产的会计处理所经常涉及的流程不同于其他固定资产的监管及程序。IT 资产包括硬件和软件以及用户的桌上计算机和工作站,这些资产都是现今技术环境中重要投资。

资产管理流程对财务报告认定的影响:

(1)资产应在财务报表中予以正确列报。这意味这资产已根据公认会计准则(GAAP)其当的予以资本化或记作费用,且已经对所有资产租赁作出适当的会计处理。此外,任何及所有要求的披露均已在财务报表中呈报。

(2)资产余额可透过观察或其他一些途径进行周期性披露,以验证它们的存在。此外,需对资产的账面值进行周期性评估、并审核相关资产类别的预计可使用年限是否合理。

(3)资产的存取以适当方式予以保护,从而合理保证任何报告日期下资产的存在。

四、总结与展望

随着我国市场经济的发展,经济信息化的日趋成熟,我国的企业将面对更加激烈的市场竞争环境,建立信息环境下良好的内部控制制度有助于我国企业在未来激烈的竞争中求得生存和发展。信息环境下的内部控制,对人、机都提出了更高的要求。萨班斯(SOX)旨在规范用于企业信息的内部控制。确保用来生成报告的数据是准确的并且不能通过任何方法来操纵是 CEO 的法定义务。它从 CEO 开始,从那里依次向下传递。反过来 CEO 将依赖 CIO 以确保 IT 过程和控制是符合遵从性检查的,而 CIO 将反过来依赖 IT 经理,IT 经理将最终依赖 DBA(Database Administrator),来确保数据处于控制之下并且是安全的。因此,我们要以 IT 的视角更新内部控制观点,打破传统,从基础控制和应用控制两方面着手,真正做到“两手抓,两手都要硬”。

参考文献:

1. Fujitsu Services, IT Governance-The Future of Control, 2002, (11).

2. Armour, Internal Control: Governance Framework and Business Risk Assessment at Reed

3. IT Governance Institute, COBIT 3rd Edition Control Objectives, 2000, (7).

4. Ron Weber, Information Systems Control and Audit, Prentice Hall. Inc., 1999, (10).

5. Victor Bennett、Bob Cancilla, IT responses to Sarbanes-Oxley, www.ibm.com, 2005-12-15.

6. KPMG, Sarbanes-Oxley section 404: management assessment of internal control and proposed auditing standards, 2003, (3).

7. 道格拉斯·R·卡迈克尔. 审计概念与方法. 大连:东北财经大学出版社, 1999.

8. Larry F. Konrath. Auditing a Risk Analysis Approach. 北京:中国人民大学出版社, 2004, (10).

9. Sally Chan, Mapping COSO and COBIT for Sarbanes-Oxley Compliance, 2002.

10. T. Hoffman, The Sarb-Ox Shift, in Computerworld, 2005 35.

11. PricewaterhouseCoopers, The Use of Spreadsheets and Considerations for Section 404 of the Sarbanes-Oxley Act, PricewaterhouseCoopers LLP, Newark, Del, 2004.

基金项目:福建省教育厅社会科学研究项目“我国财务会计信息化发展方向研究”(项目号:JA08003S)支持。

作者简介:庄明来,厦门大学管理学院教授、博士生导师;周元元,厦门大学管理学院会计系博士生。

收稿日期:2011-08-20。