会计信息系统建设中的风险控制与防范

——基于外部监管及信息系统审计视角

史振生　张爱芹

当今，企业运营大多依靠信息系统的支持，而企业信息系统尤其是会计信息系统是否安全可靠已成为企业内部控制和风险防范的重要内容。对于上市公司来说，需要满足监管机构有关信息披露及内控管理等多方面的监管要求，而且，政府及上市公司监管机构都已出台了对信息系统风险控制的法规，同时，信息系统审计组织也非常重视对信息系统的审计，并制定了许多审计标准。然而，信息系统的风险一般都是在信息系统建设过程中就已埋下的，因此，在进行会计信息系统建设的过程中，必须重视外部监管要求，并借鉴信息系统审计的风险控制思想和标准，加强风险控制与防范。

一、《萨班斯——奥克斯利法案》对会计信息系统风险管理的要求

会计信息系统是企业编制财务报告及对外披露会计信息的重要基础系统，其是否安全可靠，关系到企业是否能够按照政府及监管部门的要求，按时、完整、准确、公允披露企业经营状况及会计信息，因此，各国政府及监管机构都对企业信息系统风险控制提出了较高的要求。

2001年，安然公司会计丑闻发生之后，美国出台了《萨班斯—奥克斯利法案》(以下简称SOX)，要求上市公司的管理层建立一套有关财务报告的内部控制体系。该法案在内部控制上的要求细化到了企业运营的每个层面，其中包括与账务相关的每一个环节。

SOX涉及所有影响财务报表生成的其他业务部门，其中影响较大的是IT部门。SOX法案有一些条款是与IT直接相关的，包括Sec. 302对财务报告的提供，Sec. 404对内控报告的提供，Sec. 409实时披露材料的变更，Sec. 802为审计和评审员保留相关的记录等。对IT部门而言，遵循SOX方案，要求IT部门支持公司高管、财务和内外部审计人员的需求，以确保影响财务报表的业务流程、应用和信息基础设施的完整性、可用性和可审计性，保证内控报告和内控程序的完成，并能够对外部审计需求做出积极响应。

为遵从SOX方案，保证会计账务、财务报告、财务流程、财务应用和IT基础结构的完整性、可用性和准确性，要求IT在以下三方面有所准备：

1、优化财务流程，完善会计信息系统。在财务应用的基础上，要实现财务数据整合和统计分析，引进全面预算管理、绩效管理、财务预警等模块，保证企业提供准确、完整、实时、真实的财务报告。

2、建立内部控制体系并引入内控管理信息系统。SOX要求企业高管加强对内控程序和内控报告的责任，要求CEO和CFO能够证明年度和季度财务报告没有差错和遗漏现象，要求企业记录并检查企业的内部控制情况，揭露任何“严重弱点”，要求企业高层能够判断与业务过程相关的风险，以及这些风险对公司财务报告可能产生的影响。达到上述要求的核心内容是建立起遵从SOX的企业内控管理信息系统。内控管理信息系统至少应实现下述功能：①能够创建和记录企业内部业务流程，使公司的CEO、CFO、员工和审计人员能够实时识别、分配、测试并监视内部控制与流程，确保业务流程根据内控标准执行，一旦系统发现违反行为，将向有关人员自动报警。②能够收集并监视控制信息，使管理人员快速查看流程、组织、控制和风险的实时状态，提示管理人员注意控制目标是否实现。③为了帮助企业更好地了解和跟踪风险，内控管理信息系统应为企业建立一个能够与企业的每项业务过程相关联的风险库，一旦识别出潜在风险，内部控制管理系统能够允许企业设计控制以降低风险。

3、加强IT控制。SOX法案要求企业的内控活动，不论是人还是信息系统的操作流程都必须明白地定义并保存相

关记录，对审计过程也有存档的要求。因此，对影响财务报告的信息系统的IT控制，也是SOX内部控制的核心之一。

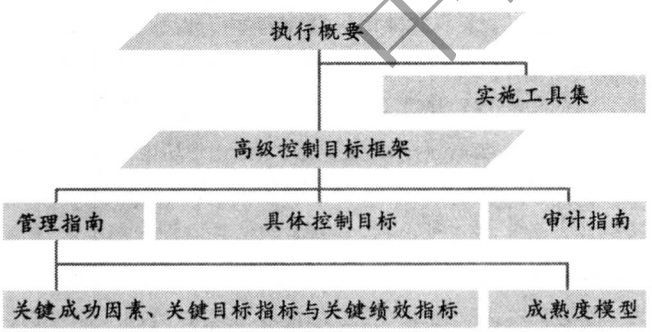
二、相关IT审计标准可为会计信息系统风险管理提供借鉴

信息系统审计(IT审计)，作为一种强化内部控制和风险管理的重要手段，成为企业识别、计量、管理和防范IT风险，保障信息系统安全的有力措施。因此，借鉴内部控制思想以及信息系统审计的体系和方法，并将其应用于会计信息系统建设中，对于防范和降低会计信息系统风险、提高企业IT治理水平具有比较重要的意义。

COBIT——信息及相关技术的控制目标，是IT治理的一个开放性标准，由美国IT治理研究院开发与推广。IT业务流程是COBIT关注的焦点，对每一个IT业务流程，COBIT提出了一系列的控制目标、相应的实现这些控制目标的控制程序等。该标准为IT的治理、安全与控制提供了一个普遍适用的公认标准，以辅助管理层进行IT治理。目前已在世界100多个国家的重要组织与企业中运用，指导这些组织有效利用信息资源，有效地管理与信息相关的风险。

COBIT架构的主要目的是为业界提供关于IT控制的清晰策略和良好典范。该架构的四个领域分别是：规划与组织(PO)、获得与实施(AI)、交付与支持(DS)和监控(Monitoring)。并进一步细分为制定IT战略规划、确定信息体系结构等34个IT处理流程。COBIT产品家族分类如图所示。

1、管理指南。其中：成熟度模型用来决定每一个控制



图：COBIT产品家族（资料来源：ISACA）

阶段和期望水准是否符合标准规范；关键成功要素用来辨认在信息化过程中实现有效控制所必需进行的活动；关键目标指标用来定义关键目标的绩效衡量标准；关键绩效指标用来测量IT控制程序是否能达到目标。以上管理方针都是为了确保企业能成功和有效地整合业务流程与信息系统。

2、执行概要提供了让管理层了解COBIT关键概念和原则的综合性简介，还概述了COBIT四大领域的体系架构。

3、目标框架详细描述了制定IT战略规划、确定信息体系结构等34个控制目标，并指出了企业对信息标准的要求和在IT资源上的需求是如何融入控制目标中的。

4、审计指南提供了关于34个控制目标的审计步骤，以协助信息系统审计师检验IT程序是否符合控制目标，并提供管理上的保证和改进建议。

5、具体控制目标为IT控制提供了一个用来明晰策略和实施指导的关键方针，包括控制目标的详细说明。

6、实施工具集包括管理意识、IT控制诊断、应用指导、常见问题等。这些新工具主要是让COBIT的应用更容易，让企业能快速且成功地掌握COBIT的应用。

需要指出的是，COBIT可具体应用到所有企业信息系统中，包括会计信息系统的建设。现在国际上已经形成了一些较为完整的IT治理的规范，如COBIT、信息技术基础结构库(ITIL)、信息安全管理标准(BS7799)等。其中，COBIT是信息系统审计与控制协会提出的IT治理的控制框架。ITIL则与COBIT紧密一致，它能够实现IT的规范化管理，记录和控制IT的基本信息，包括对网络、硬件、网页、应用、防火墙、信息系统访问控制权限、访问密码等信息，保证财务报告的IT基础结构的业务持续，帮助公司更有效监督和管理IT风险。

三、会计信息系统建设中应加强内控和风险防范意识

在会计信息系统建设中，加强内控和风险防范意识是控制会计信息系统风险的关键，而在此过程中，应树立有效、健全的信息系统内部控制的一些基本理念。

1、将业务控制要求嵌入到会计信息系统中。信息技术的应用特别是信息系统和网络技术的应用对企业的内部控制制度的建设有较大的影响：包括内部控制的观念、内涵、重点、实现手段等。在建立信息系统时，随着企业业务流程自动化程度的提高，对业务的传统控制活动逐渐被嵌入到计算机程序中。计算机代替员工来完成对业务的各种控制，业务控制的有效性依赖于信息系统的安全性、可靠性和有效性。也就是说，传统的业务控制已经转变为信息系统中的一种自动的控制。因此，企业在进行会计信息系统的建设时，必须考虑、研究和设计内控过程的嵌入，以实现企业各业务流程、会计工作流程、信息流程和内控流程的集成。

2、加强对会计信息系统本身的控制。首先，业务流程的自动化使得会计业务处理和控制的正确性和有效性依赖于信息系统的一致性和完整性。其次，信息处理和会计数据

SaaS平台
——自助式会计信息系统的应用分析

孙光国 胡仁昱 陆 政

现今市场上财务软件名目众多，由此也带来了较多的问题，比如产品质量参差不齐、产业恶性竞争等，同时也导致了软件行业难以整合形成完善的行业标准体系。因此，本文在此提出一个比较新的概念——ASP自助会计信息系统及其下一步的演变SaaS(Software as a Service，软件即服务)平台，并且从更实际的角度来讨论其未来在我国的应用。

(一)SaaS平台——自助式会计信息系统的最新实现手段

自助式会计信息系统(ASP)，就是让每一个用户按照自己的个性需要，通过现代信息技术的强大功能，自由选择各种模块进行会计信息的收集、处理、分析等，从而达到满足用户对会计信息系统多元化的要求。ASP自1999年首次在我国提出之后，国内一些知名的软件企业不断探索，将开发ASP模式的会计信息系统作为追求的目标，并取得了长足的发展。

随着互联网技术的进步，基于Internet的自助式会计信息系统的实现形式从原有的ASP模式逐步向SaaS模式演变，二者的区别主要在于技术实现层面，对自助式会计信息系统的业务层面没能太大影响。与ASP模式类似，SaaS在线会计管理平台通过Internet提供软件，用户不用再购买软件，而改用向提供商租用基于Web的软件来管理企业的经营活动，且无需对软件进行维护，服务提供商会全面管理和维护软件。对于中小企业来说，它消除了企业购买、构建和维护基础设施和应用程序的繁琐，无疑更便捷。

(二)SaaS相对于目前传统财务软件的优势

1、成本低。以租赁的方式使用软件，按需使用，按需付费，不用一次性支付大笔资金，总体成本和投资风险都大大降低，且后期升级与维护可及时免费获得。

2、方便快捷。与传统软件相比，saas在线会计不用安装软件，只要连上互联网即可使用，即理论上在任何一台能够上网的电脑上都能随时使用。后期提供免费升级和维护服务，由服务提供商在服务器端统一升级，若使用中遇到问题还可以在线咨询。

3、安全保证。由于SaaS在线会计管理平台是将客户数据存储于中央服务器，由供应商统一维护，降低了数据遗失的风险，且从技术和服务器集中管理上提供多层安全保护。相对于一般的网上财务而言，安全性大大增强。

(三) SaaS可预见的应用范围

的集中化使得会计信息系统被破坏时所造成的损失不可估量。最后，信息技术的特点决定了会计信息系统具有易被攻击的特点。所以，对会计信息系统进行有效控制是企业开展正常生产经营活动的前提和保障。

3、管理层重视是会计信息系统风险控制的重要前提。有效的会计信息系统控制需要企业管理层的重视。许多人认为会计信息系统控制只是一个技术问题，应该由技术人员负责。事实上，会计信息系统控制需要企业上下各级组织机构和各类员工的参与，需要制定并实施严格的规章制度。如果企业管理层不能够充分认识信息技术的风险，不能给以会计信息系统控制足够的重视，企业对会计信息系统控制的投资不足，而且不能动员相关人员来重视和参与会计信息系统控制，各种关于会计信息系统控制的规章制度的实施将会遇到较大的困难，进而影响会计信息系统控制的有效性。

(作者单位：中国银行总行财务管理部
河北经贸大学会计学院)

责任编辑 刘黎静