基于COBIT的信息系统审计框架研究

张文秀[a],齐兴利[b],黄溶冰[a]

(南京审计学院 a.国际审计学院;b.法学院,江苏 南京 210029)

摘 要:随着信息系统的迅速发展和广泛应用,信息系统审计作为一门新兴的交叉学科而受到较多关注。我国信息系统审计缺乏对规范体系的理论研究,而国际上多个审计组织已提出COBIT、GTAG、GAIT、FISCAM 、ITIL、BS7799、COSO等一系列与信息系统审计相关的国际准则与指南。结合我国信息系统审计的特点和国际准则的先进思想而构建的基于COBIT的信息系统审计框架以信息系统控制目标为核心,分为面向系统的信息系统审计和面向数据的信息系统审计两大范畴。

关键词:信息系统审计;COBIT;审计准则;审计框架

中图分类号:F239.1 **文献标识码**:A **文章编号**:1672-8750(2010)04-0029-06 **收稿日期**:2010-04-01

作者简介:张文秀(1975—),女,山西汾阳人,南京审计学院国际审计学院审计系讲师,博士,主要研究方向为信息系统审计、内部审计;齐兴利(1963—),女,黑龙江哈尔滨人,南京审计学院法学院书记,教授,主要研究方向为政府审计、社会审计;黄溶冰(1972—),男,黑龙江佳木斯人,南京审计学院国际审计学院副院长,副教授,博士,主要研究方向为系统工程、资源审计与资源政策评估。

基金项目:教育部人文社会科学研究课题(09YJA630073);南京审计学院校级课题(NSK2009/B18)

在信息系统(Information System)向复杂化、大型化、综合化和网络化方向发展的过程中,信息系统的可用性、保密性、完整性和有效性已经引起用户的高度重视。但是,受到用户自身能力等诸多因素的限制,信息系统用户自己难以验证信息质量,无法对信息系统的抗风险能力作出准确评估,他们迫切需要在第三方独立专业机构的帮助下,提高信息系统资产的安全性,确保业务数据的完整性,提高系统的整体效率及合法性、合规性。因此,由独立审计师收集并评估证据,以判断信息系统是否有效做到保护信息资产、维护数据完整、完成既定目标且耗用资源最少的信息系统审计应运而生。随着经济管理与信息技术的不断结合与日益渗透,跨越传统审计理论、信息系统管理理论、行为科学理论和计算机科学四个科学领域的信息系统审计,作为多学科融合的交叉学科,已成为国内外的一个研究热点。

一、信息系统审计准则的发展现状

作为全球信息系统审计的领导者和主要推动者,国际信息系统审计与控制协会(Information System Audit and Control Association,简称ISACA)推出了一系列信息系统审计准则、职业道德准则等规范性文件,并把焦点集中于信息系统保障、控制、安全和IT管理等主题上,发布了《信息及相关技术的控制目标》(Control OBjectives for Information and related Technology ,简称COBIT)[1]。国际内部审计师协会(Institute of Internal Auditors,简称IIA)制定了《全球技术审计指南》(Global Technology Audit Guide,简称GTAG)和《IT风险评价指南》(Guide to the Assessment of IT Risk,简称GAIT)。美国审计署(GAO)发布了《联邦政府信息系统控制审计手册》(Federal Information System Controls Audit Manual,简称FISCAM)。英国、

加拿大、澳大利亚、日本等国的相应机构也先后颁布信息系统审计准则和审计指南，如指导有效 IT 服务的《信息技术基础构架库》(Information Technology Infrastructure Library，简称 ITIL) 和国际信息安全管理标准 BS7799/ISO17799 等。

我国的信息系统审计研究尚处于起步阶段，相关研究比较零散。石爱中副审计长 2008 年在五届三次理事会暨第二次理事论坛上的报告曾指出：科学、完整、系统的信息化审计方法几乎还是空白[2]。胡晓明也认为我国信息系统审计研究很不完整、不系统，还没有一套成形的规范理论结构，他指出信息系统审计理论结构框架的要素应包括信息系统审计概念、目标、职能、依据、风险、技术、流程[3-4]。唐志豪提出的信息系统审计理论结构模型由信息系统审计本质、目标、规范等六要素组成[5]。卢红柱从实践探索出发研究信息系统审计的现实定位、关注操控流程和技术方法，指出需加强相关法律、规程、标准和指南的确立与完善[6]。

目前，我国在信息系统审计方面的规定或准则主要有 2001 年发布的《关于利用计算机信息系统开展审计工作有关问题的通知》、2004 年发布的《独立审计具体准则第 20 号——计算机信息系统环境下的审计》、2006 年发布的《中国注册会计师审计准则第 1633 号——电子商务对财务报表审计的影响》、2008 年发布的《内部审计具体准则第 28 号——信息系统审计》等。从这些规定的具体内容来看，我国基本停留在对信息系统环境下会计信息的审计阶段，计算机仅是一种辅助审计工具，缺乏对信息系统自身的审计。我国的信息系统审计准则研究主要集中在对 ISACA 颁布的信息系统审计准则体系和 COBIT 的分析及应用，而对其他机构颁布的信息系统规范的研究较少。如陈婉玲、马良渝等人对 ISACA 信息系统审计准则体系进行了分析[7-8]，陈婉玲、袁若宾研究了 COBIT 的构成和内容及其基本应用[9]，王会金、刘国城分析了 COBIT 在中观经济主体信息系统重大错报风险评估中的应用[10-11]。

我国政府有关部门要以科学发展观为指导，顺应信息系统复杂化、大型化、综合化和网络化的发展方向，采用科学方法，借鉴国际先进经验与成果，结合我国现状与特点，参照《审计署 2008—2012 年审计工作发展规划》，从关注信息系统整体的安全、风险、管理、控制角度，加强相关制度和规范的建设[12]，加快制定信息系统审计标准、指南与程序等，建立完善的信息系统审计规范体系。

二、信息系统审计的国际准则

信息系统审计准则是一个规范化的管理框架，它把信息系统、审计人员和被审计单位各自的权利、义务和责任等纳入管理框架，解决了各方因为职责不明确而影响信息系统质量的问题。

世界各国的多个机构和组织提出了不同的信息系统审计准则，如 COBIT、GTAG、GAIT、FISCAM 、ITIL、BS7799 等。

1. COBIT

COBIT 于 1996 年 4 月公布，目前最新版本是 2007 年 5 月 8 日发布的 4.1 版。该标准由 ISACA 的 IT 治理学会(IT Governance Institute，简称 ITGI) 在总结了多国专家的经验和 ISO9000 等标准的基础上进行开发和推广。它把 IT 业内的活动组织成为普遍接受的流程模式，是一个基于控制、关注业务、面向过程、度量驱动的控制架构。目前，COBIT 是国际上公认的最先进、最权威的安全与信息技术管理和控制的标准，已在全世界一百六十多个国家的重要组织与企业中得到运用，指导其有效利用信息资源，有效管理与信息相关的风险。

COBIT 由执行概要(Executive Summary)、框架(Framework)、执行工具集(Implementation Tool Set)、管理指南(Management Guidelines)、控制目标(Control Objectives) 和审计指南(Audit Guidelines) 六部分组成。它通过对信息系统整个生命周期活动的 IT 过程来管理 IT 资源，指导组织有效管理与信息相关的风险，从而有效实现 IT 目标。

2. 其他相关国际准则

常见的与信息系统审计有关的国际准则还有 GTAG、GAIT、ITIL、BS7799、COSO 等。

IIA 新制定的系列 GTAG 用于指导首席审计执行官(CAE)、审计委员会和审计主管解决有关信息技术管理、控制和安全方面的问题。从 2005 年 3 月 IIA 颁布第一个指南《GTAG－1：IT Controls》以来，目前共发布了 13 个成熟的信息系统审计指南，涉及信息技术控制、变更和补丁管理控制、持续审计、信息系统审计管理、管理和审计隐

私风险、管理和审计信息系统薄弱点、信息技术外包、审计应用软件控制、确认和存取管理、业务连续性管理、制定 IT 审计计划、实施 IT 审计项目、舞弊的自动化预防与侦测等方面。IIA 的高级技术委员会已选定下面几个主题作为将要发布的 GTAG，包括审计安全治理、用户开发的应用程序审计、技术产品开发生命周期审计、IT 治理、计算机辅助审计技术[13]。

IIA 于 2006 年 11 月 29 日审议通过的 GAIT 是一套基于风险的 IT 一般控制评价的原则和方法。随着国际内部审计专业实务框架（International Professional Practices Framework，简称 IPPF）的发布，GAIT 成为 IIA 强烈推荐的信息系统审计指南。GAIT 帮助企业识别合理范围内信息系统一般控制中的关键因素和关键控制点，帮助评价企业信息系统控制的成本收益以及效率效果，以满足企业遵守《萨班斯-奥克斯利法案》404 条款的要求。GAIT 实践指南包括基于风险的 IT 一般控制评估方法论、IT 一般控制缺陷评估、商业与 IT 风险三个部分[14]。

1999 年美国 GAO 发布了最初的 FISCAM，2009 年 2 月它在 2008 年 7 月草案基础上发布了最新的 FISCAM。FISCAM 提供了联邦政府和其他政府机构开展信息系统控制审计的方法指南，体现了美国国家标准与技术研究院（National Institute of Standards and Technology，简称 NIST）和公认政府审计准则（Generally Accepted Government Auditing Standards，简称 GAGAS）的审计准则与控制标准，并与 2001 年 7 月 GAO 和完整高效总统委员会（President's Council on Integrity and Efficiency，简称 PCIE）联合发布的《财务审计指南》（GAO/PCIE Financial Audit Manual）相一致。FISCAM 采用自上而下、基于风险的方法对信息系统开展基于过程的一般控制、应用控制和用户控制的审计，并关注网络环境下的安全问题，可以很好地与财务审计、绩效审计相结合[15]。

ITIL 即信息技术基础构架库，是一套被广泛认可的用于有效的 IT 服务管理的实践准则。它是英国政府商务办公室逐步提出和完善的一套对 IT 服务的质量进行评估的方法体系。ITIL 旨在提高 IT 资源的利用率和服务质量，可适用于不同规模、不同技术和不同业务需求的组织。2001 年英国标准协会正式发布了以 ITIL 为核心的英国国家标准 BS15000。

BS7799/ISO17799 是国际信息安全管理标准体系，它包括两大部分，即按照英国国家标准局制定的 BS7799 - 1《信息安全管理实践规范》和 BS7799 - 2《信息安全管理体系规范》。它以分析机构和企业面临的安全风险为起点，对企业的信息安全风险进行动态的、全面的、持续改进的管理，帮助组织建立一个初步的、易于实施和维护的管理框架，在框架内通过安全管理标准，为组织提供在信息安全管理各环节上的一个最佳的实践指导。BS7799 - 1 已于 2000 年 12 月被国际标准化组织采纳，成为 ISO17799。

COSO 框架已正式成为美国上市公司内部控制框架的参照性标准。COSO 关注整合问题，它能确认内部控制的三大主要目标，即运营的效率和效果、财务报告的可靠性以及遵守适用的法律和规章的情况。此外，该标准将控制环境、风险评估、控制活动、信息和沟通、监控作为框架的五大组成要素服务于上述三大目标。

3. COBIT 与其他准则的关系

COBIT 与 GTAG、GAIT、FISCAM 、ITIL、BS7799、COSO 等准则虽然是由不同的国家、组织和机构研究和发布，侧重面有所不同，但总的说来，这些国际准则在一定程度上体现了趋同性，其关注点主要集中在控制、安全和服务。COBIT 注重学习和借鉴业内已有的相关准则的优点，注重和其他准则的结合。

GAIT、FISCAM 与 COBIT 的角度比较接近，都是针对信息系统的控制，GAIT 主要关注一般控制，FISCAM 则包括一般控制与应用控制两大方面。ITIL、BS7799 和 COSO 分别是针对 IT 服务、信息安全和内部控制的，又各有一套方法和体系。COBIT 在修订的过程中注重学习和吸收世界上其他先进的标准与方法，将其融合到自身的结构中，加强了 COBIT 基于风险的 IT 一般控制、IT 服务、信息安全和内部控制等方面，并允许用户根据其特点与需求，将 COBIT 与 GTAG、GAIT、FIS CAM、ITIL、BS7799、COSO 等有机地结合，从而更好地实现信息系统审计目标。

三、我国信息系统审计框架的构建

构建信息系统审计框架，将便于人们加深对信息系统建设与应用过程的理解，指导审计机构

建立相应的机制，将信息系统建设与应用的全部过程置于有效的管理与控制之下。

1. 参照准则的选择

在众多信息系统审计国际准则中，本文认为应该选择 COBIT 作为主要参照。这是因为 COBIT 与其他准则相比具有以下优势。

首先，COBIT 的体系结构比较系统。COBIT 特有的三维三层体系结构较其他相关国际准则更具系统性。COBIT 框架将 IT 过程、IT 资源及信息、企业的策略与目标联系起来，形成一个三维的体系结构。三维体系中具有清晰的层次：最上层是执行概要，专门为资深管理层解释 COBIT 的关键概念和原则；第二层是控制目标，“自上而下”地根据域、过程、任务活动三个层次对总体目标进行分解，确定了 318 个具体控制目标，并给出详细的系统管理策略、措施及注意事项等；第三层是指导实务的管理指南、审计指南和应用工具集，提供了管理与审计的工具与方法，定义了度量模型，并围绕控制目标提出了相应的审计流程和改进建议。COBIT 的这种层次分明的体系结构便于从纷繁的问题中明确目标、理清思路，指导各级审计人员开展信息系统审计工作。

其次，COBIT 的内容比较完善。多个信息系统审计相关准则中，GAIT、FISCAM 主要集中在信息系统控制上，ITIL 关注于 IT 服务，BS7799 针对信息安全，COSO 则从内部控制的角度出发，而 GTAG 颁布时间较短，还处于不断完善中。COBIT 的内容覆盖信息系统整个生命周期中的各个过程，可指导开展基于风险的过程导向的信息系统审计，涉及 IT 治理、内部控制、IT 服务、信息安全等多方面。而且，COBIT 能够与其他信息系统审计准则较好地融合，它在特定的领域显得更加完善。

最后，COBIT 的国际认可度较高。COBIT 经过十余年间多个版本的完善，从 1.0 版局限于审计，经过 2.0 版关注控制、3.0 版关注管理，发展到 4.0 版上升至治理的高度，体现了信息系统审计研究和发展的过程。目前 COBIT 的最新版本 4.1 已比较成熟。GTAG、GAIT 等发布时间不长，而 FISCAM 的主要对象为政府机构，ITIL、BS7799、COSO 等应用范围也有明确限定。因此，在多个信息系统审计准则中，COBIT 的国际认可度最高，已在全世界一百六十多个国家和地区的重要组织与企业中得到运用。我国在信息系统审计的研究与发展中，应尽量借鉴国际成功经验，实现与国际惯例接轨。

2. 构建思想

我国信息系统审计框架的构建，一方面要以 COBIT 等信息系统审计国际准则为参考，借鉴其基于控制、关注业务、面向过程、逐层分解的控制架构，利用其现有的指南等成果；另一方面，要从我国信息系统审计研究与应用的特色出发，充分考虑技术、文化等方面的东西方差异。

我国信息系统审计框架应基于 COBIT 的思想，从系统的角度，采用自上而下的方法，以控制目标为中心，用多层次控制目标指导对信息系统的控制和审计。控制目标应按照域、过程和任务活动逐步细化，可借助 COBIT 的“控制目标汇总表”确定各个 IT 过程的具体审计目标，并通过评估被审计信息系统在各个层面上是否达到了控制标准来确定信息系统的控制风险水平。管理指南应给出度量信息系统安全、可靠与有效的指标体系，给出为管理者提供评估标准的度量模型。其中成熟度模型可以帮助确定被审计信息系统是否符合行业和国际标准，通过与行业和国际标准的比较，审计师可以了解被审计信息系统的固有风险水平。COBIT 的审计指南为评估机构或信息系统审计师对信息系统进行分析、评估和实施审计提供了建议与指导，可以直接应用于信息系统审计，对我国开展信息系统审计具有很好的启示和指导作用。

但是，我国信息系统审计框架不能照搬 COBIT。COBIT 是适用于西方文化和技术环境下的基于控制的信息系统审计体系，而我国信息系统审计是传统审计在信息化环境下的发展。我国的信息系统审计关注信息系统中数据的真实性、合法性、正确性，即我国实施的是以面向数据为主的信息系统审计，兼顾信息系统本身。我国今后的信息系统审计将以数据式审计为基础，以控制为目标，以风险为导向，加强面向信息系统本身的审计。我国信息系统审计框架需从中国国情出发，以 COBIT 中的控制目标为中心，针对信息系统中的面向系统和面向数据的控制措施，以管理指南和审计指南为指导，根据其主要涉及的是信息系统本身还是信息系统所处理的数据，分别指引我国面向系统的信息系统审计和面向数据的信息系

统审计。

3. 框架结构

本文基于对 COBIT 等信息系统审计国际准则的研究,结合我国信息系统审计研究与应用现状,提出一个适用于我国的基于 COBIT 的信息系统审计框架,如图 1 所示。

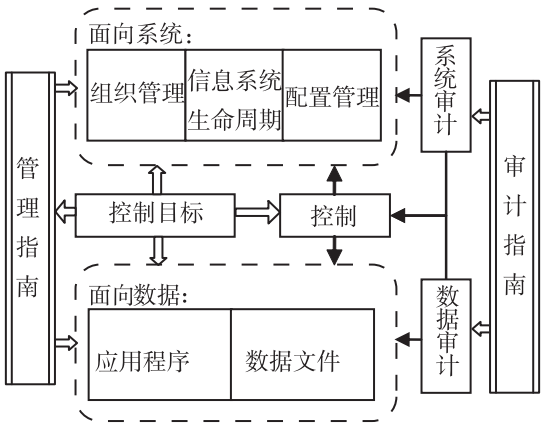

图 1　基于 COBIT 的信息系统审计框架

该框架以信息系统控制目标为核心。按照审计的范围,该框架将信息系统审计分为面向系统和面向数据两个大的范畴。参照国际惯例,将信息系统控制分为一般控制和应用控制。面向系统的审计主要是对信息系统一般控制的审计,面向数据的审计主要是对信息系统应用控制的审计。如框架所示,一方面,企业或组织可根据 COBIT 管理指南实施面向系统和面向数据的信息系统管理与控制。另一方面,信息系统审计师可根据 COBIT 审计指南设计并开展系统审计与数据审计,通过获取审计证据,来客观评价被审计单位的信息系统,并提出改进建议。

系统层面由组织管理、信息系统生命周期管理、配置管理三个部分组成。组织管理包括以风险管理为中心的进度管理、成本管理、质量管理等内容。组织管理可参照 COBIT 中的管理指南加强对进度、成本和质量的管理,并建立起度量指标和评价体系,促进组织实现目标并增加价值。信息系统生命周期管理是针对信息系统整个生命周期的,包括获取、供应、开发、运作、维护等过程,参照 COBIT 中的规划与组织、系统获得与实施、交付与支持、运行性能监控四个域开展针对 IT 过程的控制和审计。配置管理在信息系统生命周期中识别、定义包括涉及信息系统环境的所有软硬件配置项,并将其基线化,是灾难恢复与业务持续计划的基础,也为问题管理、变更管理和发布管理等提供基础。

数据层面由应用程序、数据文件两个部分组成。应用程序主要实现信息系统的数据输入、处理、输出功能,对应用程序的审计需借助多种数据校验方法和检测技术,保证应用程序控制是健全有效的,保证程序编码的正确性、有效性,从而实现完整、准确的数据处理。数据文件是信息系统中原始数据、处理的中间结果和最后结果的存储所在文件,对数据文件的审计就是要实现对信息系统当中数据的真实性、正确性、完整性、合法性、安全性进行评价。信息系统审计师根据 COBIT 控制目标确定对应用程序和数据文件的审计需求,参照管理指南和审计指南完成数据审计任务。

我国急需制定与完善有关信息系统审计的准则与指南。在制定信息系统审计准则时,需广泛而深入地研究国际信息系统审计准则,借鉴它们的先进理念和成功经验,但同时也要注意文化、技术、工具等方面的差异。本文提出的基于 COBIT 的信息系统审计框架是一个在我国当前信息化条件下对 COBIT 及其他相关国际准则的应用研究,在引进 COBIT 等国际准则的先进思想与体系的同时,又能实现与我国信息系统审计的实际情况相结合。本文力图推动我国信息系统审计的研究与应用的进一步深入。

参考文献:

[1] ISACA. Control objectives for information and related technology V4.1 [EB/OL]. [2009 - 04 - 20]. www.itgi.org/cobit.

[2] 石爱中. 加强审计理论研究——坚持审计实践,注重研究方法[EB/OL]. [2008 - 03 - 20]. http://www.chinaaudit.org.cn/news_show.asp? id = 1313.

[3] 胡晓明. 信息时代的 IS 审计理论结构构建[J]. 中南财经政法大学学报,2006(3):108 - 111.

[4] 胡晓明. 我国信息系统审计的发展战略研究[J]. 学习与探索,2005(5): 204 - 206.

[5] 唐志豪. 信息系统审计理论结构研究[J]. 财会月刊:理论,2007(3): 59 - 61.

[6] 卢红柱. 计算机信息系统审计的探索之路[J]. 审计研究,2006(增刊): 12 - 20.

[7] 陈婉玲,杨文杰. ISACA 信息系统审计准则及其启示[J]. 审计研究,2006(增刊): 108 - 112.

[8]马良渝,潘婉霞. ISACA 信息系统审计准则体系浅析[J]. 中国管理信息化,2007(3):69-71.
[9]陈婉玲,袁若宾. COBIT 及其在信息系统控制与审计中的应用[J]. 审计研究,2006(增刊):93-96,104.
[10]王会金,刘国城. COBIT 及其在中观经济主体信息系统审计的应用[J]. 审计研究,2009(1):58-62.
[11]王会金,刘国城. 中观经济主体信息系统审计的理论分析及实施路径探索[J]. 审计与经济研究,2009(5):27-31.
[12]中华人民共和国审计署. 审计署 2008—2012 年审计工作发展规划[EB/OL]. [2009-04-19]. http://www.audit.gov.cn/n1057/n1087/n1779/1607101.html.
[13]IIA. Global technology audit guides (GTAG)[EB/OL]. [2009-12-04]. http://www.theiia.org/guidance/standards-and-guidance/ippf/practice-guides/gtag/.
[14]IIA. Guide to the assessment of IT risk(GAIT)[EB/OL]. [2009-12-13]. http://www.theiia.org/guidance/standards-and-guidance/ippf/practice-guides/gait/.
[15]GAO. GAO federal information system controls audit manual (FISCAM) GAO-09-232G [EB/OL]. [2009-12-13]. http://www.gao.gov/special.pubs/fiscam.html.
[16]中国内部审计协会. 内部审计具体准则第 28 号——信息系统审计[S]. 2008.
[17]金文,张金城. 基于 COBIT 的信息系统管理、控制与审计的模型构建研究[J]. 审计研究,2005(4):75-79.
[18]徐瑾. 基于信息化环境下数据式审计的特征与实施路径[J]. 审计与经济研究,2009(1):50-55.
[19]张金城,黄作明. 信息系统审计[M]. 北京:清华大学出版社,2009.
[20]Hall J A. 信息系统审计与鉴证[M]. 李丹,刘济平,译. 北京:中信出版社,2003.

(责任编辑:杨凤春)

On Information System Audit Framework Based on COBIT

ZHANG Wen-xiu[a], QI Xing-li[b], HUANG Rong-bing[a]
(a. School of International Audit; b. School of Law,
Nanjing Audit University, Nanjing 210029, China)

Abstract: With the rapid development and extensive application of information systems, more and more attention is given to Information System Audit which is an emerging cross-discipline. Many international auditing organizations have issued their standards and manuals, such as COBIT, GTAG, GAIT, FISCAM, ITIL, BS7799, COSO, etc, while the research of information system audit standards is few in China. This paper analyzes the structures, contents and connections of these different standards and manuals, and then studies information system audit standards and guidelines. Combining China's national conditions with the advanced thinking of COBIT, it proposes a COBIT-based framework for Information System Audit.

Key words: information system audit; COBIT; audit standards; audit framework