借鉴ISACA出版物完善我国信息系统内部控制规范体系

阳 杰　应里孟

（温州大学城市学院　浙江温州　325035）

【摘要】在我国信息系统内部控制规范体系建设伊始，借鉴国际上相关机构制定的相关规范和最新动态，是我们立足国情、有的放矢地开展规范制定的基础。在国际上众多规范制定机构中，信息系统审计与控制协会（ISACA）的出版物的内容相对专业和完整，可资借鉴。

【关键词】信息系统审计　COBIT　规范体系

一、我国信息系统内部控制规范的现状

2005年6月，财政部、国资委和证监会向国务院联合上报了《关于借鉴<萨班斯法案>完善我国上市公司内部控制制度的报告》，并获国务院同意。2006年，上海证券交易所和深圳证券交易所分别出台了《上市公司内部控制指引》，国资委也颁布了《中央企业全面风险管理指引》。之后，我国于2008年5月发布了《企业内部控制基本规范》，并在2010年4月发布了配套的《企业内部控制应用指引》、《企业内部控制评价指引》和《企业内部控制审计指引》。其中，《企业内部控制应用指引》是主体，是对企业按照内部控制原则和内部控制五要素建立、健全企业内部控制，是对18项具体经济业务所提供的指引。财政部还针对每个指引进行了详细的解读，这其中就有专门针对信息系统的《企业内部控制应用指引第18号——信息系统》，该指引是基于COBIT框架构建起来的，是对信息系统整个生命周期实施的控制。《企业内部控制评价指引》着眼于帮助企业管理层对企业内部控制进行自我评价，并且专门对内部控制评价报告进行规范。《企业内部控制审计指引》是注册会计师和会计师事务所执行内部控制审计业务的执业规范。这三个指引是对《企业内部控制基本规范》内容的细化，目的是增强它的可操作性。总的来说，我国的内部控制规范体系基本成型。

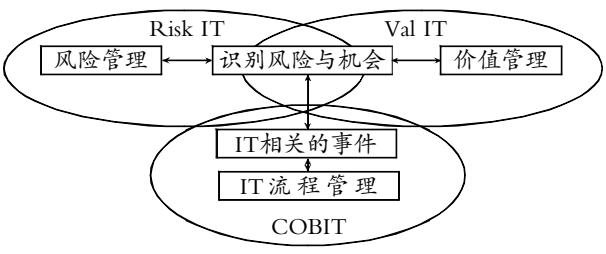
不过，在我国目前大力推广会计信息化的背景下，与信息系统相关的内部控制规范体系则还处于酝酿构建之中。2008年11月12日，财政部会同九部委以及相关行业、企业共同成立了会计信息化委员会暨XBRL中国地区组织，旨在为推进我国会计信息化建设提供组织保障、协调机制和智力支持。在成立大会上，提出了开展会计信息化标准体系建设的要求。财政部于2009年4月12日正式发布了《关于全面推进我国会计信息化工作的指导意见》（财会[2009]6号），其再次确认了建立会计信息化标准体系的要求。在XBRL标准体系初步建立之后，下一步会计信息化标准体系建设的工作重点将是信息系统内部控制规范体系的建设。

在国际上众多相关规范制定机构中，ISACA围绕信息系统审计、控制、风险管理和治理出版了一系列的规范和指导材料，其内容相对专业和完整，可作为完善我国信息系统内部控制规范体系的参考。

二、ISACA的出版物概览

ISACA专门致力于信息系统内部控制、审计和治理相关规范的开发，它所开发的规范和相关出版物充分借鉴了全球相关领域出版物的精髓，并且将它们进行整合、拓展和创新，使得ISACA的出版物具有权威性，被全球数千家大型企业广泛采用，许多国家在制定相关规范时，也以ISACA的出版物为蓝本。所以，我们需要对ISACA的出版物系列有一个清楚的了解。

迄今为止，ISACA开发的框架有五个：信息及相关技术控制目标框架（COBIT）、IT价值框架（Val IT Framework）、IT风险框架（Risk IT Framework）、IT认证框架（IT Assurance Framework，ITAF）和用于信息安全的业务模型（Business Model for Information Security，BMIS）。其中，IT价值框架和IT风险框架是COBIT的拓展，并成为COBIT的补充性框架。IT价值框架着眼于如何进行IT投资决策，以及如何实现投资收益。IT风险框架着眼于帮助管理者管理与IT相关的风险。由于IT所带来的风险和价值是一体两面的，因为不存在没有风险的价值，风险管理的结果也是为了更好地创造价值，所以，IT风险管理和IT价值管理框架通常在针对同一个IT活动的时候，是相互联系和相互补充的，它们都将IT活动与业务目标建立联系，着眼于受托责任、平衡风险和创造价值。这三个框架的关系如下图所示。



COBIT、IT风险框架、IT价值框架的关系图

值得注意的是，由于ISACA的框架和出版物众多，这给大家造成理解和整合方面的困难，目前正在开发的COBIT5.0试图将COBIT4.1与ISACA在其他领域的研究和开发（例如价值、风险、安全、确认）进行整合，以期提供一个一致的和集成的指南的来源。COBIT将会实现COBIT4.1和Val IT2.0以及Risk IT的结合，同时还会将BMIS和ITAF的部分内容囊括其中。这种整合将有助于克服出版物众多导致的内容难以整合的问题（ISACA，2010）。

（一）COBIT框架及相关出版物

COBIT框架开始建立的目的就是消除审计师、业务管理人员和IT管理人员之间的沟通鸿沟，因为他们往往对于同一个问题所采用的专业术语及其对问题的理解并不一致，COBIT因此成为沟通业务领域和IT领域的桥梁。经过数年的演进，COBIT已经将全球主要的IT标准融汇其中，成为IT治理、管理和认证领域使用最为广泛的框架，它提供了企业使用信息和相关技术的完整视角。COBIT能够帮助企业董事会、执行层、董事和管理层理解和指导重要的IT相关的需求，对关键的IT活动进行监督和评价，进而做出有理有据的决策。ISACA和它下属的IT治理委员会（ITGI）围绕COBIT出版了一系列的出版物，它们设计用来支持企业实施有效的IT治理，并且给IT安全领域、IT治理领域和IT认证领域的专业人员提供指导。

1.《董事会关于IT治理的指示（第2版）》（Board Briefing on IT Governance，2nd Edition）描述了IT治理的概念，指出了ISACA的五个IT治理关注领域，并提供了关于对IT进行治理的角色和责任，以及如何设置一个有效的IT战略委员会的指南。它还提供了一个清单和工具来帮助管理层启动和维持一个有效的IT治理计划。

2.《信息安全治理：给董事会成员和执行管理层的指导（第2版）》（Information Security Governance：Guidance for Boards of Directors and Executive Management，2nd Edition）采用业务的术语来解释了信息安全，并且帮助执行人员和管理人员理解信息安全问题，并且对他们的组织正在管理安全相关的风险感到放心。

3.《ITGI支持ISO/IEC 38500：2008采纳的白皮书》（ITGI Enables ISO/IEC 38500：2008 Adoption）。ISO/IEC38500：2008是由ISO（国际标准化组织）和IEC（国际电工委员会）发布的一个IT治理标准。ITGI发布的这个白皮书的目的就是认识到了ISO38500标准的出版需要一个有效的指导和支持，如何应对ISO38500中的相关原则和概念，以便有效地对它进行采用。该白皮书描述了ISACA产品家族如何提供这种指导，并且采用一种可以根据组织规模进行"量体裁衣"的方法。

4.《实施和持续改进IT治理》（Implementing and Continually Improving IT Governance）对先前的ISACA的《IT治理实施指南：使用COBIT和Val IT（第2版）》（IT Governance Implementation Guide Using CobiT? and Val ITTM，2nd Edition）的内容进行了提升、拓展和改进。它包含ISACA出版的研究前沿方面的有价值的参考。这份指南采用了一种实施团队可以采用一种有效和高效的方式来实施IT治理的方法，并且建立了一个基于持续改进生命周期、用于实施和维护有效的IT治理的良好实践方法，这可以根据企业的特定需求进行量身订制。

5.《COBIT控制实务：实现用于成功IT治理的控制目标的指导（第2版）》（CobiT Control Practices：Guidance to Achieve Control Objectives for Successful IT Governance，2nd Edition）提供了关于为什么需要控制，以及满足具体控制目标的控制实务。这份指南可以确保所提出来的解决方案会更加完整和成功的实施。COBIT控制实务提供了支持控制目标的关键控制机制。

6.《COBIT安全基准（第2版）》（CobiT Security Baseline，2nd Edition）。采用一种容易遵照进行的方式，提供了一个企业采纳一个IT治理框架所需的信息，主要关注的是IT安全的具体问题方面。它提供了一个关于信息安全的介绍，同时揭示了安全的重要性，以及基于COBIT的安全基准和关键控制。该指南还包括了对ISO/IEC 27002的参考。

7.《发现价值：执行人员对IT治理关键角色的入门》（Unlocking Value：An Executive Primer on the Critical Role of IT Governance）用于帮助执行者理解如何发现他们对IT的投资所产生的优势，同时交付可靠的解决方案。它给执行者提供了一个如何应用良好的管理实务的理解，也包括了如何建立一个号召企业采纳IT治理的概念的需求。

8.《萨班斯-奥克斯利法案的IT控制目标（第2版）》（IT Control Objectives for Sarbanes-Oxley，2nd Edition）是在SOX要求下，为执行管理层和IT控制专家对一个组织的IT控制进行评价的时候提供参考。该出版物提供了在IT环境中，如何基于COBIT中与财务报告相关的控制目标来确保对SOX的遵循的指南。

9.《用于巴塞尔协议的IT控制目标》（IT Control Objectives for Basel II）提供了一个在巴塞尔协议背景下，用于管理运营和信息风险的框架。它提供了一个对巴塞尔协议下的风险、运营风险和IT风险之间的关联以及用于管理信息风险方法的概览。

10.《IT认证指南：使用COBIT》（IT Assurance Guide：Using CobiT）介绍了当前存在的各种类型的IT认证活动，并且描述了COBIT如何被用于支持这些活动。它提供了一个给认证专业人员的指南，同时提供了一个与COBIT框架相连接的结构化的认证方法。这样，它提供了一个用于业务和IT人员的共同的语言和标准。

11.《COBIT快速启动（第2版）》（CobiT Quickstart，2nd Edition）是一个用于中小规模企业进行IT治理的基准，在这些企业中，IT在战略重要性方面要求并不高，或者IT对于企业的生存而言并不关键。快速启动指南也可以作为大型企业在追求一个适当水平的IT控制和治理实务的起点。快速启动指南包含一个对COBIT资源的总括的视角，设计用来帮助快速和容易地采用COBIT的大多数的必要的要素。它关注与大多数的关键IT流程、控制目标和指标，并且采用一种容易参照的格

式,来帮助用户快速获取COBIT的收益。

12.《COBIT和应用控制：对管理层的指导》(CobiT and Application Controls：A Management Guide) 提供了一个关于应用控制的指导,包括定义和特征,以及对应用控制的设计和运行,这些应用控制与其他控制(例如,IT一般控制)之间的关系和依赖,以及业务和IT管理者的相关责任。

13.《COBIT映射文件》(CobiT Mapping Papers)，该指南包含COBIT与其他国家和行业标准之间的映射关系,还包括了由ITGI出版的相关框架与COBIT框架之间的映射。这些映射包括COBIT与ISO/IEC 27002，NIST SP 800-53，ITIL，TOGAF，CMMI,PMBOK与PRINCE2之间的对应关系。

14.《理解业务目标如何驱动IT目标：对执行者的说明》(Understanding How Business Goals Drive IT Goals：Executive Briefing)，该指南是来自一些业务部门的专家小组被要求将一组业务目标和IT目标进行评估、排序和联系的一个主要的结果。该研究结果产生了用于IT的业务目标,以及COBIT中相关的IT目标。

15.《建立用于COBIT和Val IT的商业案例》(Building the Business Case for CobiT and Val IT：Executive Briefing),这是对COBIT和Val IT的商业价值的探索和论证。研究所产生的大量数据集提供了许多的分析机会，除弄清对IT的企业治理和业务绩效之间的关系之外，它也提供了一个关于当前在不同规模、行业部门和地理位置的企业中,实施COBIT和Val IT框架的一个现状。

16.《将CobiT 4.1与ITIL v3和ISO/IEC 27002相对应获取商业收益》(Aligning CobiT 4.1，ITIL v3 and ISO/IEC 27002 for Business Benefit),这是英国商务部所开展的一个联合研究的结果，它提供了一个如何将CobiT 4.1、ITIL v3和ISO/IEC 27002进行协调、实施和整合的最佳实务。ITIL v3是英国商务部开发的一个IT服务管理框架,ISO/IEC 27002是国际标准化组织制定的信息安全管理实用规则。

17.《给服务管理者提供的COBIT用户指南》(CobiT User Guide for Service Managers)，是对服务管理者面临的业务和治理方面的挑战,以及COBIT如何可以用于帮助应对这些挑战的一个介绍。它解释了服务管理者的角色,以及它对于一个进行有效的IT治理的重要性的解释。它还解释了与ITIL V3流程和COBIT4.1控制目标之间的角色对应的关键治理任务、案例,一个用于该角色领域的高层成熟度模型,以及和其他参考物之间的联系。

(二)Val IT系列出版物

1.《企业价值:对IT投资的治理,VAL IT框架2.0》(Enterprise Value：Governance of IT Investments，The Val IT? Framework 2.0)是COBIT的一个辅助框架,包含了关键的管理流程和实务,还包括了用于以下三个领域的成熟度模型:价值治理、资产管理和投资管理。

2.《给认证专家的价值管理指南：使用Val IT 2.0》(Value Management Guidance for Assurance Professionals-Using Val IT 2.0)基于《IT认证指南:基于COBIT》,提供了关于如何使用Val IT来支持一个认证评价，关注的是对基于IT的业务投资的治理。

3.《企业价值:对IT投资的治理——商业案例》(Enterprise Value：Governance of IT Investments，The Business Case)涵盖了用于开发一个有效的商业案例的八个步骤（建立情况说明书,一个生命周期的视角的现金流概览,考虑协同问题,风险评价,对风险和回报的优化),同时还提供了用于每一个步骤的有用的工具。它也提供了一个适当的商业案例内容的完整的概览。

4.《Val IT映射:Val IT2.0与MSP,PRINCE2和ITIL V3之间的映射》(Val IT Mapping：Mapping of Val IT 2.0 to MSP? PRINCE2?ITIL? V3)。Val IT并非在真空中运行的,当前存在一些其他的准则和最佳实践的出版物，它们可以用于如何管理企业的IT项目和计划中的具体的方面。该出版物提供了Val IT2.0与MSP、PRINCE2和ITIL V3之间的映射关系。它给实务人员指明了这些框架如何进行互补，如果能够将这些框架综合使用,效果会更好。

5.《企业价值:IT投资治理——从价值管理开始》(Enterprise Value：Governance of IT Investments，Getting Started with Value Management)列出了如何实施Val IT框架,并提供了针对企业投资方面的建议。

6.《商业案例指南：使用Val IT 2.0》(The Business Case Guide：Using Val ITTM 2.0)，这份指南是基于Val IT 2.0框架,给业务和IT执行者、组织领导者、业务发起者和程序管理者的提示。该信息帮助专业人员从“为什么(why)”开始,通过“是什么(what)”,再到“如何(how)”构建、维护和使用商业案例作为一个运营工具。

(三)Risk IT系列出版物

1.《IT风险框架》(The Risk IT Framework),这是COBIT的一个辅助性的框架,并且包含关键的管理流程、实务和成熟度模型,用于三个领域:风险治理、风险评估和风险响应。

2.《IT风险实务人员指南》(The Risk IT Practitioner Guide)是《IT风险框架》的一个支持性出版物,它提供了可以用于应对IT相关风险问题的关键技术的例子，还提供了关于如何应用IT风险流程模型中的概念的详细指导。该指南指出如何使用COBIT和Val IT来降低风险,还将《IT风险框架》与ISO31000、ISO27005 和COSO ERM进行了比较。

(四)IT认证框架(ITAF)

信息技术认证框架(ITAF)是一个完整和良好的实务集合模型,它提供了关于设计、执行和报告IT审计和认证安排的指南;定义了IT认证相关的术语及概念;建立了针对IT审计和认证专业人员的角色和责任、知识和技能、勤勉尽责、执行和报告要求。ITAF关注ISACA的材料，也包括ITGI和其他组织所开发的指南,因此,提供了一个给IT审计和认证专业人员可以寻找指南、研究政策和程序、获得审计和认证项目、开发有效报告的统一来源。虽然ITAF包含现有的ISACA准则和指南,但它已经被设计成一个“活文档”,随着新指南的开发和发布,它们将会在该框架中建立索引,而且可以供ISACA成员使

用。ITAF由三类准则（一般准则、执行准则和报告准则）、指南、工具和技术组成。

1. 一般准则是IT职业界执业的指导性原则。它们应用于开展所有的任务，针对IT审计和认证职业界的道德、独立性、目标和应有关注，也包括知识、胜任能力和技能。

2. 执行准则是针对任务的具体开展，例如计划和监督、范围确定、风险和重要性、资源利用、监督和任务管理、审计和认证证据，以及运用专业判断和应有关注。

3. 报告准则针对的是报告的类型、沟通的途径，以及所需要沟通的信息。

4. 指南给IT审计和认证职业界提供了关于一个审计或者认证领域的信息和指引。与上面三类准则一致，指南关注的是各类审计处理方式、方法、工具和技术，以及在计划、执行、评估、测试和报告IT流程、控制和相关的审计或者认证活动的相关材料。指南也帮助界定企业的活动和措施（activities and initiatives），以及那些由IT来执行的活动和措施之间的关系。

5. 工具和技术提供了关于各种方法、工具和模板的详细信息。在该指南中，还提供了对这些方法、工具和模板的使用，以及使用它们来进行信息操作。工具和技术是直接与具体的指南建立联系的。它们采用各种形式，例如讨论文档、技术指引、白皮书、审计程序或者书籍，以及ISACA的SAP出版物，还提供了支持ERP系统的指南。

（五）用于信息安全的业务模型（BMIS）

BMIS是采用一个整合的方法来管理信息安全，并且提供了一种用于信息安全专业人员和业务管理者讨论信息保护的共同语言。该模型包含四个要素（组织设计和战略、人员、流程和技术）和六个动态的相互关系（文化、架构、治理、突然事件、许可与支持、人员因素）。该模型的特点在于：以业务为导向，可以用于不同规模的企业；除了关注技术，还关注人员和流程；它独立于任何特定的技术，可以应用于所有的行业、国家、规章和法律系统；包含了传统的信息安全，并且建立了与隐私、风险、物理安全和合规之间的联系；能够让信息安全专业人员将安全计划与业务目标进行协同。

三、完善我国信息系统内部控制规范体系的几点建议

第一，我国目前已经制定的与信息系统内部控制相关的规范中，《企业内部控制应用指引第18号——信息系统》已经借鉴了COBIT框架，但它的控制还停留在一般控制层面，对应用控制并没有涉及，这可以借鉴ISACA的COBIT框架中所提到的六个应用控制，以及《COBIT和应用控制：对管理层的指导》来进行补充性规定。

第二，对信息系统审计而言，我国内部审计协会发布的《内部审计具体准则第28号——信息系统审计》也是停留在原则性的规定上面，对于具体的实施缺乏指导。我们建议结合ISACA的ITAF框架来制定更加细化的规定。

第三，我国的《企业内部控制评价指引》要求企业根据基本规范、应用指引以及本企业的内部控制制度，围绕内部环境、风险评估、控制活动、信息与沟通、内部监督等五要素，对内部控制有效性进行全面评价，包括财务报告内部控制有效性和非财务报告内部控制有效性。这与国际惯例要求的对财务报告内部控制进行单独评价不同，事实上在信息系统中，我们已经很难从纷繁复杂的信息系统内部控制中剥离出与财务报告相关的内部控制。在我国目前企业内部能够执行信息系统内部控制评价的人员极其匮乏的情况下，企业迫切需要相关的具有可操作性、易参照的指南，这绝非《企业内部控制应用指引第18号——信息系统》一个指引能够满足企业的现实需求。所以，我们建议会计信息化委员会成立专门的任务小组，对ISACA的出版物进行充分的借鉴吸收，从安全、风险、控制、价值和治理五个角度制定细化的指导材料。

第四，针对内部控制的具体要素制定相应的指南。COSO和ISACA对内部控制监控要素的关注值得我们借鉴，根据我国的《企业内部控制基本规范》中的要素进行细化的指导，对于内部控制的具体实施很有必要。在这方面，ISACA《COBIT控制实务：实现用于成功IT治理的控制目标的指导（第2版）》可以提供参考。

第五，目前我国信息安全标准的建设尚属空白。ISACA的《用于信息安全的业务模型》、《COBIT安全基准（第2版）》和《信息安全治理：给董事会成员和执行管理层的指导（第2版）》给我们提供了这方面的参考。

第六，考虑IIA制定的全球技术审计指南。至今，IIA已经发布了与信息技术相关的15项全球技术审计指南（GTAG）。IIA的GTAG是从业务的视角来提供高层技术信息，帮助内部审计师更好地理解关于IT的风险、控制和治理问题，它更加注重概念方面的阐述，而对于技术细节却没有太多涉及。这和ISACA着重于“实战”形成鲜明的对比。除此之外，IIA还发布了《IT风险评估指南》（GAIT），它提供了在“自上而下、风险基础”的审计方法中，确定IT一般控制范围的原则和方法。

第七，最好规范制订规划。我们发现，ISACA制定框架有一个由点到面、从分散到集中的过程。也就是说，它是根据实务领域中的应用经验，根据需求不断地增加新的准则、指南或者框架。随着对相关领域的认知加深，ISACA会将相关联的材料进行整合，用一个更加全面的框架来进行管理。我们的建议是，在我国制定信息系统内部控制规范的过程中，可以根据国际上的先进经验建立框架，根据需求的轻重缓急来逐步对框架进行完善，这样有助于避免我国各个准则制定机构之间工作之间的冲突。

主要参考文献

庄明来，阳杰.美国IT控制的审计规范体系解读与启示.经济管理，2009；11