企业 IT 内部控制评价

方 耀

指导教师 庄明来教授

厦门大学

学校编码：10384　　分类号_____密级 _____

学号：X2007157014　　UDC _____

厦门大学

硕 士 学 位 论 文

企业 IT 内部控制评价

Study on IT Internal Control Assessment of Enterprise

方 耀

指导教师姓名： 庄 明 来 教授

专 业 名 称： 会计硕士(MPAcc)

论文提交日期： 2015 年 4 月

论文答辩日期： 2015 年 月

学位授予日期： 2015 年 月

答辩委员会主席：_____

评 阅 人：_____

2015 年 4 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“ √ ”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

内容摘要

信息技术（Information Technology，以下简称 IT）内部控制是企业内部控制的有机组成部分，是由董事会、监事会、经理层和全体员工，针对信息系统实施的控制，以合理地保证企业内部控制目标的实现。它对企业内部控制目标、要素等方面造成了重大影响。随着 IT 在企业中得到越来越广泛的应用，为防范其带来的风险，IT 内部控制系统的建设、运行和评价引起越来越多的关注，并成为企业内部控制评价的重要内容。这要求企业持续改进 IT 内部控制评价体系，以实现内部控制目标。

本文首先分析了 IT 对内部控制带来的影响、IT 内部控制的重要性，以及 IT 内部控制目标和评价体系的特点。在考察国内外的相关理论文献，以及现有与 IT 相关的主要内部控制规范基础上，针对目前国内缺少权威的 IT 内部控制实施和评价的规范，现有的规范难以指导企业的实践之现实，构建了基于信息及相关技术控制目标（Control Objectives for Information and Related Technology， COBIT）框架的内部控制评价指标体系，进而运用流程能力模型，评价 IT 内部控制的有效性。同时根据在评价公司层面 IT 内部控制时，该指标体系具有多层次性和模糊性的特点，选择采用模糊综合评价法进行评价。在评价时，笔者使用层次分析法确定各层次指标的权重，将定性指标量化，并根据量化的得分评价企业 IT 内部控制的执行有效性和设计的完整性。除此之外，在梳理 A 公司 IT 内部控制建设、运行的现状和 IT 内部控制评价的基础上，对评价结果进行了分析，以期对我国政府监管部门、中介机构和实施企业 IT 内部控制建设和实施提供指导性建议。

关键词：企业；IT 内部控制；评价

Abstract

Information Technology (hereinafter referred to as IT) internal control is an organic part of the enterprise internal control, and it is operated targeted at information system by the board of directors, supervisory board, management and all other members of staff in order to ensure reasonably the realization of the enterprise internal control objectives. It had material effects on many aspects such as the internal control objectives, elements etc. With the more and more extensive applications of IT in the enterprise, for the prevention of the risks, the establishment, operation and the assessment system of the IT internal control has been given more and more attention and becomes an important content of internal control assessment. This requires enterprise to improve the assessment system of IT internal control and achieve the internal control objectives.

This paper firstly analyzed the effects of IT on internal control, importance of IT internal control, and the characteristics of IT internal control objectives and assessment system. After the study of the relevant theoretical literatures both at domestic and foreign and main existing internal control standards associated with IT, I find that our country lacks authoritative IT internal control standards of implementation and assessment and the existing standards are not sufficient to guide practice. Therefore, based on the COBIT framework, assessment index system of internal control is constructed to evaluate the effectiveness of the IT internal control with Process Capability Model. Because the index system is of multi hierarchy and fuzziness, when evaluating the IT internal control of company level, we take Fuzzy Comprehensive Evaluation Method to evaluate and use Analytic Hierarchy Process to determine the weight of index of various levels and quantify the qualitative indicators, and then I evaluate the effectiveness of enterprise IT internal control implementation and completeness of design according to the quantitative score. Based on IT internal control establishment, current situation of operation and

assessment situation of IT internal control of A company in the analysis, combined with the assessment results are analyzed. On this basis, this paper puts forward the guiding suggestions of establishment and implementation of IT internal control on the Chinese government supervision departments, intermediaries and the implementation enterprises.

Key words: enterprise; IT internal control; assessment

目录

Contents

第一章　导论

1.1　研究的背景和意义

当今，信息已成为所有企业的关键资源，随着计算机信息技术的日益进步，信息系统已经渗透到公共和商业环境的每一个角落。通常所说的信息系统是指由一系列相互关联的组件构成，用于采集、处理、储存和发送信息，以支持组织的决策和控制[①]。限于篇幅，本文讨论的信息系统都是基于现代计算机及网络信息技术构建的。这里提到的“组件”包括计算机和网络基础设备、应用系统、数据、信息、系统的用户和相关的规章制度。一方面，现代社会高度依赖着信息系统的支撑。信息系统自信息创建之日到信息销毁之时，无不发挥着重要的作用。该系统虽在组织中不从事某一具体的实物性工作，却像神经系统一样使组织得以协调一致。它的开发和建立使企业摆脱了落后的管理方式，将管理工作统一化、规范化、现代化，极大地提高了管理的效率，信息系统已成为企业最有价值的资产。但另一方面，我们应清醒地意识到，鉴于信息系统本身的复杂性和高风险特征，它时刻面临着巨大的威胁和风险。假如我们对相关威胁控制不力，必然会导致信息系统负面效应的产生。当信息系统不能按照设计要求工作或运行时，大量依赖信息系统的公司将会严重丧失其商业价值；信息系统管理不当所导致的信息泄漏或毁损，对组织及社会必然产生严重的后果。我们把由于信息系统的薄弱点而造成的信息资产甚至其他相关资产损失的潜在可能性称为信息系统风险。信息系统风险随着企业的信息系统与业务耦合度的不断加强而攀升。多数企业已经认识到，必须高度重视信息系统风险并加以防范，但实际上，失败的案例却数不胜数。为此，企业无疑应当高度重视信息技术（Information Technology，以下简称 IT）的内部控制，建立 IT 内部控制系统，并评价其是否有效。

本文以企业的信息系统风险为出发点，在对国内外 IT 内部控制相关理论、规范进行研究的基础之上，对 IT 内部控制的评价内容进行分析，借鉴国际广泛认可的信息及相关技术控制目标（Control Objectives for Information and

[①]引自肯尼思·C·劳东，简·P·劳东，劳帼龄译.管理信息系统[M].北京：人民大学出版社，2009.P9.

Related Technology，以下简称 COBIT）框架构建内部控制评价指标，提出评价的方法，并引入实施 IT 内部控制方面有较多经验的企业案例加以说明。本文希望能为企业的 IT 内部控制评价体系提供理论借鉴和具体的实务参考,有助于企业完善 IT 内部控制；进而强化 IT 治理，强化风险管理，防范企业风险。

1.2 研究内容与思路

本文立足于企业 IT 内部控制评价，通过理论探讨和案例分析给出 IT 内部控制评价方法。论文首先梳理 IT 内部控制及评价的相关规范和文献，分析了国内外 IT 内部控制及评价规范；进而选取了 COBIT 5 框架为基准构建评价体系。在此基础上,本文选取A电信公司开展IT内部控制建设和评价的案例加以分析，利用模糊综合评价法和层次分析法对公司层面 IT 内部控制整体效果进行评价，提出改进该公司 IT 内部控制的若干建议。在此基础上对政府监管部门、中介机构和实施企业提出建议。本文的整体结构如图 1－1 所示。

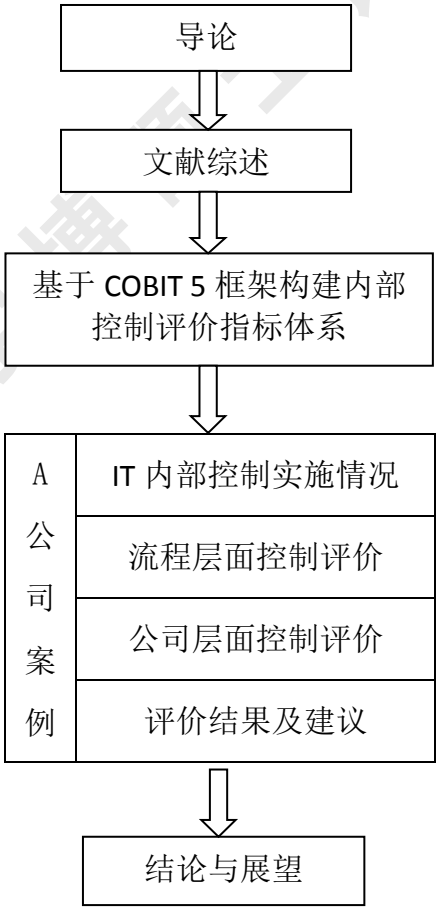

图 1－1：论文基本框架图

1.3　论文研究方法

本文采用规范研究与实证研究相结合的研究方法，通过搜集、阅读和整理国内外与 IT 内部控制相关的框架、文献，基于应用视角对文献进行归类与分析，梳理出研究方向。参考国际先进的 COBIT 5 框架，构建评价公司层面 IT 内部控制的指标体系。在此基础上，通过 A 公司的案例分析，验证了本文所提出的 IT 内部控制评价方法的科学性与可行性。

同时，本文还采用模糊综合评价法，把定性指标加以量化，进而评价公司层面的 IT 内部控制。本文侧重于模糊综合评价的基本方法与技术，结合案例，采用层次分析法计算 IT 内部控制各指标的权重，将多目标、多因素的无结构内部控制指标系统化、结构化，建立起不同层级指标的递阶式层次关系。然后运用 COBIT 5 的流程能力模型，以定量的方式表示 IT 内部控制实施有效性和设计完整性的评价结果，客观地评价企业 IT 内部控制质量。

1.4　论文贡献与不足

1. 论文贡献

（1）本文较为系统地梳理了基于 COBIT 框架的 IT 内部控制评价方法。当前对 IT 内部控制的研究甚多，但大多是从外部审计的角度探讨内部控制要素评价，对企业如何评价自身的 IT 内部控制体系研究较少。至今，我国尚未形成一套公认权威的 IT 内部控制评价体系。本文尝试将 COBIT 模型运用到企业 IT 内部控制评价中去，较为系统地补充和完善现有的评价体系，为构建完整的 IT 内部控制评价体系提供理论支持。

（2）运用模糊综合评价法设计 IT 内部控制综合评价模型。目前对 IT 内部控制的评价主要是基于 COSO 内部控制框架（以下简称 COSO）或《企业内部控制应用指引第 18 号——信息系统》（以下简称信息系统应用指引）进行定性的要素评价，而从定量角度对企业 IT 内部控制总体评价研究甚少。本文力求通过量化方法，为更准确、客观地对企业进行 IT 内部控制评价提供参考。

2. 论文不足

论文中设计的 IT 内部控制整体评价指标具有一定的通用性，但由于不能确