中国会计学会
ACCOUNTING SOCIETY OF CHINA

财政部重点会计科研课题系列丛书(2010)

Internal Control in Information Technology

信息技术内部控制

操作指引与典型案例研究

中国会计学会 编

林 斌 覃 东 信息技术内部控制操作指引与典型案例研究

大连出版社
DALIAN PUBLISHING HOUSE

中国会计学会
ACCOUNTING SOCIETY OF CHINA

财政部重点会计科研课题系列丛书(2010)

Internal Control in Information Technology

信息技术内部控制

操作指引与典型案例研究

中国会计学会 编

林 斌 覃 东 信息技术内部控制操作指引与典型案例研究

大连出版社
DALIAN PUBLISHING HOUSE

图书在版编目(CIP)数据

信息技术内部控制操作指引与典型案例研究/中国会计学会编. —大连:大连出版社,2010.6

(财政部重点会计科研课题系列丛书. 2010)

ISBN 978-7-80684-942-2

Ⅰ. ①信… Ⅱ. ①中… Ⅲ. ①企业管理—管理信息系统—研究 Ⅳ. ①F270.7

中国版本图书馆 CIP 数据核字(2010)第 108442 号

出 版 人:刘明辉
策划编辑:毕华书 周 鑫
责任编辑:张丽娜
责任校对:金 石
封面设计:金啸宇
版式设计:金啸宇
责任印制:徐丽红

出版发行者:大连出版社
地址:大连市西岗区长白街 10 号
邮编:116011
电话:(0411)83627430/83621349
传真:(0411)83610391/83620941
电子信箱:bhs@dlmpm.com
印 刷 者:大连美跃彩色印刷有限公司
经 销 者:各地新华书店

幅面尺寸:170mm×240mm
印 张:11
字 数:221 千字

出版时间:2010 年 7 月第 1 版
印刷时间:2010 年 7 月第 1 次印刷
印 数:1~2000 册
书 号:ISBN 978-7-80684-942-2
定 价:22.00 元.

如有印装质量问题,请与我社营销部联系
购书热线电话:(0411)83627430/83621049

财政部重点会计科研课题
评审委员会

主　任　刘玉廷

副主任　应　唯　刘光忠　李玉环　周守华

委　员（以汉语拼音为序）

陈汉文　戴德明　方红星　付　磊　高一斌
耿建新　江建平　李建发　李心合　李玉环
刘光忠　刘明辉　刘宵仑　刘玉廷　刘志远
陆建桥　陆正飞　曲晓辉　宋献中　汤谷良
唐建华　田志心　王　斌　王光远　王　宏
王化成　王立彦　魏明海　夏冬林　谢志华
徐经长　杨世忠　杨晓舟　杨有红　应　唯
俞明轩　喻　灵　张　蕊　张宜霞　郑洪涛
支晓强　周守华　朱海林　朱荣恩

序

为落实中国会计学会第七届理事会科研规划，繁荣中国的会计理论研究，中国会计学会组织实施了财政部重点会计科研课题（2008）的研究。本次重点会计科研课题是针对我国企业内部控制和会计准则建设以及理论研究中出现的亟待解决的重点、难点问题等予以立项的，共有25个课题项目、59个课题组中标。

中国会计学会对所有立项课题进行了严格的跟踪管理。经过近一年的认真研究，绝大部分课题组较好地完成了课题预期的研究任务。自2009年3月开始，中国会计学会先后在北京、南京、南昌等地召开了4次课题结项鉴定会，与会专家对本次重点课题的研究成果给予了充分肯定，同时对每一份研究报告提出了具体的修改意见。根据报经财政部批准的课题评审结果，已有49个课题研究报告通过评审，其中14个课题被评为优秀。

为及时推广本批课题的理论研究成果，推动中国企业的内部控制建设和发展，进一步完善会计准则体系，更好地为我国改革和发展服务，中国会计学会特选出部分优良的课题研究报告，作为“财政部重点会计科研课题系列丛书（2010）”予以出版。

中国会计学会组织的财政部重点会计科研课题（2008）研究，得到了金蝶软件有限公司和大连出版社的资金支持，特此致谢。

中国会计学会

2010年3月

目　录

■ 信息技术内部控制操作指引与典型案例研究

（课题主持人：林斌　覃东）

财政部重点会计科研课题研究报告

（项目批准号:2008KJA12）

信息技术内部控制操作指引与典型案例研究

课题主持人:林　斌　覃　东

课题组成员:吴炎太　刘伟贤

刘善敏

第一章　信息系统内部控制应用指引

第一节　企业内部控制应用指引——信息系统（建议稿）

第一章　总　则

第一条　为了促进企业做好信息系统内部控制，提高信息系统安全性、可靠性、合理性，充分发挥信息系统处理业务事项、强化内部控制、改善信息沟通的作用，根据国家有关法律法规和《企业内部控制基本规范》，制定本指引。

第二条　信息系统内部控制包括一般控制和应用控制。

一般控制，是指对企业信息系统的开发和应用环境进行的控制。

应用控制，是指利用信息系统对业务处理实施的控制。

信息系统，是指在信息技术支持下，为处理企业事务、辅助企业决策，而由人员、硬件、软件、信息、运行规程等组成的集合体。

信息技术，是指在计算机和通信技术支持下，对信息进行收集、传输、加工、存储、检索、分析和输出的技术。

第三条　企业应当对信息系统相关的风险进行全面评估，至少关注涉及信息系统的下列风险：

（一）缺乏信息战略规划或者战略规划不当，可能导致重复建设、形成信息孤岛，影响企业目标的实现；

（二）信息系统建设缺乏计划或者计划不当，可能导致无法实现预期目的；

（三）设计开发不合理或者不符合需求，可能导致系统运行效率低下或者无法实现预期目的；

（四）设计开发没有实现业务控制要求，未能有效预防和发现错误和舞弊；

（五）安全措施不当，可能导致信息的泄露、篡改、毁损，造成系统无法正常运行；

（六）授权管理及职责分离不当，可能导致非法操作和舞弊；

（七）缺乏容灾、应急管理和运行维护机制，可能导致系统中断运行、信息

毁损。

第四条　企业应当对信息战略规划的制定和实施、信息系统开发和应用等环节进行全面梳理，并根据风险评估结果，明确信息系统开发和应用中的关键控制点，采取适当的控制措施对风险进行控制。

第五条　企业应当根据发展战略，结合自身的业务范围、企业文化、技术能力、组织架构、地域分布等特点，制定信息战略规划。

企业应当定期进行信息战略规划的复核，评估规划执行情况，并在必要时对规划进行调整。

第六条　企业应当考虑各信息系统的集成与共享，通过统一技术规范、加强主数据管理、共享信息系统设备等手段发挥资源整合优势，改善信息沟通，提高经营效率。

第二章　职责分工与授权审批

第七条　企业应当建立信息系统开发和应用的岗位责任制，明确相关部门和岗位的职责、权限，确保信息系统开发和应用中的不相容岗位相互分离、制约和监督。

企业信息系统开发和应用中的不相容职责至少应当包括：

（一）系统开发与验收测试；

（二）数据库管理与应用程序管理；

（三）系统管理与业务操作；

（四）系统开发与业务操作。

企业将信息系统开发和运行维护工作委托给专业服务商的，应当约定专业服务商遵循不相容职责相分离的要求。

第八条　企业应当建立信息化工作组织领导与运行体制，明确企业管理层、各部门以及下级单位的职责权限、授权批准程序和工作协调机制。

企业可以指定专门部门或岗位（以下统称归口部门）对信息系统实施归口管理，负责信息系统开发、运行维护和变更等工作。

用户部门应当根据本部门职能定位参与信息系统开发和应用。

第九条　企业信息战略规划、主要的信息系统开发和应用管理制度应当由归口部门组织制定，由董事会或类似决策机构（以下统称决策机构）批准后实施。

第十条　企业重大信息系统项目方案，应当由归口部门审查提出意见后，报决策机构批准。

归口部门在审查中应当至少关注以下问题：

（一）项目是否符合企业信息战略规划；

（二）是否存在重复建设情况，各系统的软、硬件组件可否共享或者统一采购；

（三）各信息系统的功能设计、建设进度安排是否相互协调；

（四）信息系统建设是否遵循了企业统一的技术规范，是否存在与其他系统交换信息的技术障碍。

第十一条　企业应当建立信息系统上线审批制度。对于系统上线运行和升级替换，应当由归口部门和用户部门批准后方可实施。重要系统上线和升级替换应当由企业决策机构批准后方可实施。

第三章　信息系统开发、运行维护与变更

第十二条　企业应当建立规范的信息系统开发流程制度，并定期进行复核、修订。

信息系统开发流程一般为：系统规划、需求分析、系统设计、编程、测试、上线、评价与维护。

第十三条　用户部门应当对信息系统的功能、性能、控制要求、安全性等提出明确需求，形成书面需求文档。

第十四条　系统设计方应当就总体设计方案与用户部门进行沟通和讨论，说明方案对用户需求的响应情况。存在备选方案的，应当详细说明各方案在成本、建设时间和用户需求响应上的差异。

归口部门和用户部门应当对选定的设计方案予以书面确认。

第十五条　信息系统上线前应当进行系统测试和用户验收测试，测试方应对测试结果予以书面确认。

第十六条　企业应当制定信息系统上线计划，并经归口部门和用户部门审核。上线计划一般包括人员培训、数据准备、进度安排、应急预案等内容。

培训计划应当包括对业务操作人员和系统管理人员的培训。

系统上线涉及新旧系统切换的，企业应当在上线计划中明确应急预案，保证新系统失效时能够顺利切换回旧系统。

信息系统上线涉及数据迁移的，企业应当制定详细的数据迁移计划，并对迁移结果进行测试。用户部门应当参与数据迁移过程，对迁移前、后的数据予以书面确认。

第十七条　信息系统上线后，企业应当对系统运行中的问题和系统未能满足用户需求的情况进行记录，并定期总结和分析，对系统进行调整和完善。

第十八条　企业应当定期评价信息系统负荷情况，必要时应当进行硬件设备扩容、软件系统性能优化等工作。

第十九条　企业应当建立并执行系统数据定期备份制度,明确备份范围、备份频度、备份方法、备份责任人、备份存放地点、备份有效性检查等内容。

第二十条　企业应当根据业务性质和风险程度,制定信息系统业务持续和灾难恢复计划。必要时,企业应当建立容灾中心。

第二十一条　企业应当采用日常检测、设立容错冗余、编制应急预案等预防性措施,确保信息系统的持续运行。

第二十二条　企业可能由于系统开发不完善、用户需求变动或者应用环境的变化而对已经上线实施的信息系统进行变更。对于信息系统的变更,企业应当按照本章关于系统开发的控制要求实施控制。

第四章　信息系统安全

第二十三条　企业应当根据信息系统业务性质、重要性程度、部署方式、涉密情况等确定系统的安全等级,针对不同等级采用相应的制度和技术手段确保系统安全。

第二十四条　企业应当建立用户管理制度,加强对重要业务系统的访问权限管理。

企业应当禁止不相容职务用户账号的交叉操作。

对于发生岗位变化或离岗的用户,用户部门或人力资源部应当及时通知系统管理人员调整其在系统中的访问权限或者关闭账号。

企业应当定期对系统中的账号进行审阅,避免有授权不当或非授权账号存在。

企业应当严格规定超级用户的使用条件和操作程序,并对其在系统中的操作全程进行监控或者审计。

第二十五条　企业应当采用密码控制等技术手段进行用户身份识别。对于重要业务系统,有条件的企业应当采用数字证书、生物识别等可靠性强的技术识别用户身份。

第二十六条　企业应当充分利用操作系统、数据库系统、应用系统提供的安全机制,设置安全参数,加强系统访问安全。

第二十七条　对于重要的计算机设备,企业应当禁止,必要时利用技术手段防止用户擅自安装、卸载软件或者改变软件系统配置,并定期对上述情况进行检查。

第二十八条　对于存在网络应用的企业,应当综合利用防火墙、路由器等网络设备,漏洞扫描、入侵检测等软件技术,以及远程访问安全策略等手段加强网络安全,防范来自网络的攻击和非法侵入。

对于在网络传输的涉密或者关键业务数据,企业应当采取必要的技术手段确保信息传递的保密性、准确性和完整性。

第二十九条　企业应当采取安装安全软件等措施防范信息系统受到病毒等恶意软件感染和破坏。

第三十条　企业应当对重要岗位员工进行信息系统安全保密培训，与其签署信息安全保密协议，执行泄密责任追究制度。

第五章　信息技术设备

第三十一条　企业应当根据信息系统的安全保护等级、功能及性能要求等因素，参照国家相关技术标准，建立并维护相应的信息技术设备，保证信息系统安全稳定运行。

第三十二条　企业应当将服务器等关键信息技术设备放置在合适的物理环境中，由专人负责管理和检查，任何人未经授权不得接触关键设备。

企业应当根据实际情况，通过分配钥匙、设置门禁系统权限、陪同访问、建立出入登记制度等方式保证信息系统的物理访问安全。

第三十三条　企业处置信息技术设备，应当经用户部门和归口部门确认保密信息的消除。

第三十四条　企业应当建立信息技术设备异常情况处理制度。

第六章　应用控制设计

第三十五条　企业开发信息系统，应当利用信息技术优势，优化流程，完善控制点，将处理规则嵌入到系统程序中，实现手工处理环境下难以实现的控制功能，以更加高效地预防、发现和纠正错误和舞弊。

第三十六条　企业应当根据实际情况，确定对不同控制环节采取系统控制、手工控制或者系统与手工结合控制。

对于可以完全由计算机自动处理的事项，企业应当设计为系统控制。

第三十七条　企业信息系统的权限管理功能应当满足业务职责分工的要求。

企业应当按照用户工作职责，通过信息系统中的权限管理功能控制用户的操作权限，并按照不同业务的控制要求避免将不相容职责的处理权限授予同一用户。

企业应当尽量利用信息系统自动控制业务处理中不相容职责的分离。

第三十八条　企业开发信息系统，应当针对手工录入、批量导入、接收其他系统数据等不同数据输入方式，分别考虑对进入系统数据的检查和校验功能，确保数据的准确性、有效性和完整性。

第三十九条　企业应当尽量避免通过后台操作修改和删除数据的情况。对于必需的后台数据操作，企业应当建立规范的流程制度，并对操作情况进行监控或者审计。

对于经常性的数据删除和修改，应当在系统功能中予以考虑，并通过审批、复

核等程序加以控制。

第四十条　企业应当识别信息系统中的控制参数,建立规范的管理流程,对控制参数的创建、维护进行审批控制,确保其准确性、完整性和一致性。

第四十一条　企业应当在重要的信息系统中设置操作日志功能,详细记录系统每个账户的登录时间、重要的操作内容,确保操作的可审计性。

第四十二条　对异常的或者违背内部控制要求的交易或者数据,企业应当考虑在系统中设计自动报告功能。

第二节　制定信息系统内部控制应用指引的说明

一、理论依据

《企业内部控制应用指引——信息系统(建议稿)》(以下简称本指引)根据COSO报告、COBIT框架及财政部的《企业内部控制基本规范》进行拟定。

本指引的目标依据COBIT框架的业务要求纬度确定,各章依据COBIT框架的IT资源纬度确定,各章的具体条款依据COBIT框架的IT过程纬度并结合《企业内部控制基本规范》确定。

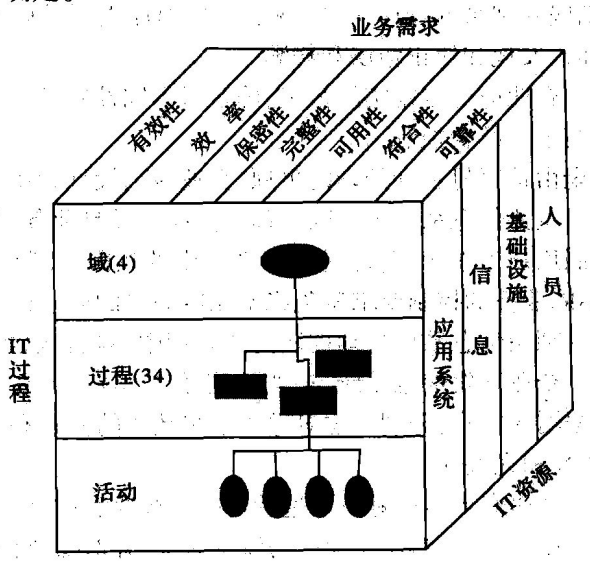


图1-1　COBIT框架体系结构

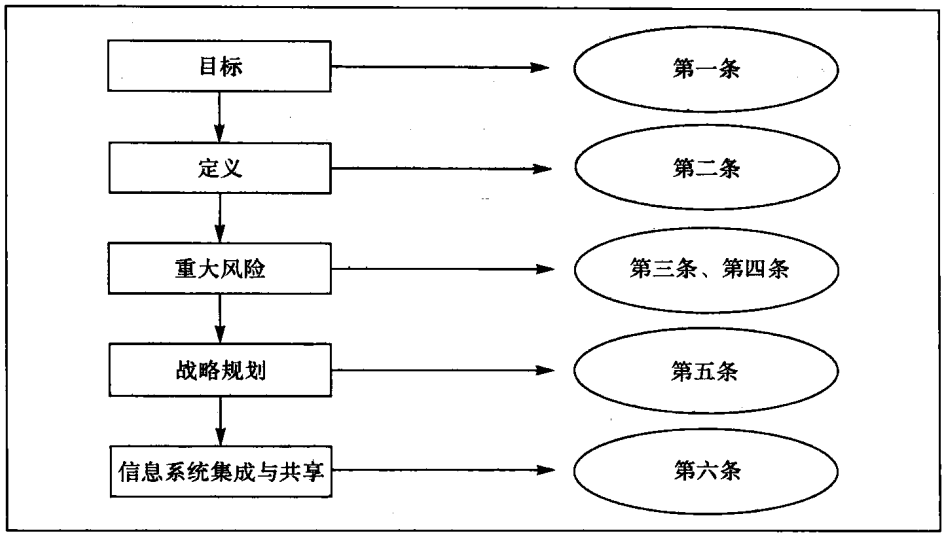
根据 COBIT 框架的业务要求，我们认为信息系统内部控制的目标是：引导企业充分利用信息系统达到企业的战略目标和业务目标，提高信息系统的效率与效益，增强信息系统的安全性、可靠性和合理性及信息的保密性、完整性和可用性，降低人为因素导致内部控制失效的可能性，形成良好的信息传递渠道。

COBIT 框架的 IT 资源包括人员、基础设施、信息和应用系统。其中，“人员”对应于指引的第二章“职责分工与授权审批”，“基础设施”对应于第五章“信息技术设备”，“信息”对应于第六章“应用控制设计”，“应用系统”对应于第三章“信息系统开发、运行维护与变更”及第四章“信息系统安全”。第一章对应于“控制环境”。

根据 COBIT 框架的 IT 过程，一方面可以得到应用系统的开发、运行维护、变更、安全管理等四个流程；另一方面要根据这四个流程的 IT 过程以及《企业内部控制基本规范》的五要素分别确定各关键风险点和控制点的具体控制条款。

二、具体条款说明

（一）第一章 总则



第一条明确了信息系统内部控制应用指引的目标。

第二条明确了信息系统一般控制和应用控制的定义。

第三条指明了信息系统开发与运行过程中的重大风险。企业在大型系统项目中由于缺乏相关管理经验，往往处于被动，如果聘请第三方为企业提供独立的质量