我国集团公司管理信息化的风险控制研究

WOGUO JITUAN GONGSI GUANLI XINXIHUA DE FENGXIAN KONGZHI YANJIU

周常兰◎著

知识产权出版社
全国百佳图书出版单位

北京服装学院专业建设项目资助出版

我国集团公司管理信息化的风险控制研究

周常兰　著

知识产权出版社
全国百佳图书出版单位

图书在版编目(CIP)数据

我国集团公司管理信息化的风险控制研究/周常兰著. —北京:知识产权出版社,2015.4

ISBN 978-7-5130-3406-7

Ⅰ.①我… Ⅱ.①周… Ⅲ.①企业集团—企业信息化—风险管理—研究—中国 Ⅳ.①F279.23

中国版本图书馆 CIP 数据核字(2015)第 056232 号

责任编辑:王 辉 责任出版:孙婷婷

我国集团公司管理信息化的风险控制研究

周常兰 著

出版发行:知识产权出版社有限责任公司 网 址:http://www.ipph.cn
电 话:010-82004826 http://www.laichushu.com
社 址:北京市海淀区马甸南村 1 号 邮 编:100088
责编电话:010-82000860-8381 责编邮箱:wanghui@cnipr.com
发行电话:010-82000860 转 8101/8029 发行传真:010-82000893/82003279
印 刷:北京中献拓方科技发展有限公司 经 销:新华书店及相关销售网点
开 本:720 mm×1000 mm 1/16 印 张:12.75
版 次:2015 年 4 月第 1 版 印 次:2015 年 4 月第 1 次印刷
字 数:190 千字 定 价:42.00 元
ISBN 978-7-5130-3406-7

前　言

管理信息化与风险控制紧密相连，管理信息化与风险控制不仅是整个企业业务的重要支撑，也是对企业运营活动进行控制的重要手段。随着管理信息化建设的逐步深入，企业的日常运营越来越依赖于 IT 系统的支撑。当前，在出现了大规模的分布式、网络化的信息技术条件下，将 IT 有效地集成到业务和信息过程中是必然趋势，我国企业的管理信息化正在进入以整合应用和加强 IT 运行维护服务管理为主要特征的新阶段，如何控制企业管理信息化的相关风险是此阶段面临的主要问题之一。

对于集团公司而言，管理信息化已经成为企业未来经营的基本条件，是集团公司的必由之路。由于集团公司经营管理的复杂，对集团公司管理信息化提出了更高的要求，不仅要求及时、准确、完整地提供以财务信息为核心的经营管理信息，而且进一步要求利用网络化信息技术手段对集团内部的各种资源进行高度集中的管理、控制和配置，并迅速地对各种财务、管理方案做出科学的、符合企业价值最大化的决策。因此，当前我国集团公司管理信息化的应用系统一般具有先进性、多元性、集成性、开放性四大特点，管理信息化本身在建设的各个阶段面临着种种风险控制问题，因此，集团公司管理信息化建设的风险控制问题尤其突出。

本书以“风险控制目标设定”→“风险控制标准”→“风险控制水平评价”→“风险应对”为基本的逻辑主线，在理论分析和实践发展历程总结的基础上，研究了当前我国集团公司管理信息化建设的风险控制目标和风险控制标准，通过对我国集团公司管理信息化建设风险控制水平的实证研究，分析了当前的风险控制状况及存在的主要问题，提出了相应的对策和建议。以期为我国集团公司加强管理信息化建设的风险控制、进行相关的合规性建设提供有价值的理论指导和实践对策。

本书是在本人博士论文的基础上修改而成的，本书的出版凝聚了各方

面的支持和关怀，首先要感谢我的导师陈宝峰教授的指导和教诲，感谢中国农业大学席爱华副教授、任金政副教授、张建胜副教授等各位师长给予的建议与帮助，感谢北京服装学院商学院的历任领导和同事给予的支持与鼓励；其次要感谢中国农业大学和北京服装学院为本项研究工作提供了资助，感谢北京服装学院专业建设（本科实践教学建设）项目为本书的出版提供了资助；再次要感谢用友集团唐肖鲁高级副总裁、国资委研究中心的张召虎先生、中国信息安全年会的主办方（《计算机世界》杂志社）为本项研究的调查提供了帮助或机会；最后还要感谢所有参与问卷调查的企业，为研究工作提供了可供参考的大量数据，正是在各方面的支持与帮助下，使得本项研究得以顺利完成。

虽然管理信息化的风险控制问题有着深入研究的必要性和迫切性，但由于这一问题的研究属于交叉领域，国内这方面的研究并不多，尚处于起步阶段和发展阶段，还有许多问题需要进一步深入研究和探索，本项研究还存在不少局限性和不足，因此，希望本书的出版能够起到一点抛砖引玉的作用。

目　录

图目录

表目录

第一章　绪论

1.1　选题背景与研究意义

1.1.1　选题背景

随着经济全球化和我国市场经济体制的建立与完善，企业集团化已经成为我国现代工商企业的基本标志。“企业发展的历史其实就是企业集团发展的历史，只有集团式的巨型企业才能真正代表一国经济的实力，真正代表市场经济的发展进程。”[106]集团公司作为独立的经济主体，是企业集团的核心企业，在全球化和市场化的背景下，面对着激烈的竞争，需要提高对各种变化的反应速度，需要提升管理水平。而管理信息化作为满足这些需要的支持手段，是企业提高核心竞争力，与国际接轨的重要途径。企业利用现代信息技术，通过信息资源的深入开发和广泛利用，不断提高生产经营、管理决策的效率和水平，进而提高企业经济效益和竞争力。因此，管理信息化已经成为企业未来经营的基本条件，成为集团公司的必由之路。集团公司经营管理比较复杂，对集团公司管理信息化的要求更高，不仅要求及时、准确、完整地提供经营管理信息，而且进一步要求利用网络化信息技术手段对集团内部的各种资源进行管理、控制和配置，并迅速地做出科学的、符合企业价值最大化的决策。

在信息技术迅猛发展和深入应用的情况下，就我国集团公司管理信息化的应用系统而言，与一般企业的相比，呈现出先进性、多元性、集成性、开放性四大特点。当前，在出现了大规模的分布式、网络化的信息技术条件下，将信息技术(IT)有效地集成到业务、信息和管理过程中成为必然趋势，

我国集团公司的管理信息化正在进入以整合应用为主要特征的新阶段，集团公司的日常运营越来越依赖于IT系统的支撑，管理信息化的相关风险正成为管理层、监管部门重点关注的对象，IT内控也逐渐成为集团公司内部控制的重要组成部分，并成为审计的对象之一。

集团公司管理信息化的各个阶段都存在风险。比如，在规划实施方面，有的企业管理信息化是“脚踩一块西瓜皮，滑到哪里算哪里”，造成系统无法集成、数据无法共享、信息资源浪费，缺乏总体规划；有的企业选择软件时“贪大求全”，结果选择贵的软件、功能齐全的软件并不适合企业业务和管理部门的真实需求；有的企业为了成功实施购买的系统，不得不放弃企业原有的一些好的管理方法，忍痛“削足适履”。在运行维护方面，自然灾害、事故、错弊、对企业不满的员工等因素都会带来各种风险，这些风险给企业、社会带来经济损失及其他危害。为此，近年来，各方面的监管层也出台了大量的规范，如《企业内部控制基本规范》《中央企业全面风险管理指引》《信息技术服务运维通用要求》《商业银行信息科技风险管理指引》《证券公司信息技术管理规范》等，都对管理信息化的相关风险做出了明确的规定及要求，企业已经进入了“合规年代”。

在这种背景下，研究当前我国集团公司管理信息化风险控制状况如何，以及应该如何加强管理信息化的相关风险的控制，以达到各监管层的相关合规性要求已经成为理论界和实务界广泛关注的问题。

1.1.2 研究意义

从理论上看，现有的研究主要是由西方国家的研究机构或学者提出来的，实证研究也大多以发达国家的企业应用特点为依据，而西方企业经历了充分的工业化发展阶段，业务和管理上经历了优化过程，一般是以最好的运行办法作为标准，以达到规范运作和高效运行的目的，并且不断地从目前的标准上升到更高的标准。因此，西方企业标准化和制度化程度一般较高，公司治理结构也比较完善，并且有较高的企业风险管理意识、经验和机制。但是，由于历史原因，我国长期处于计划经济体制下，工业革命还没有完成又遇上经济全球化的网络时代，根据后发优势理论，中国共产党的十六大报告中指出，我国实施的是“以信息化带动工业化，以工业化促进信息化”的发展战略，走的是“新型工业化路子”。其背景如图1-1[71]所示。

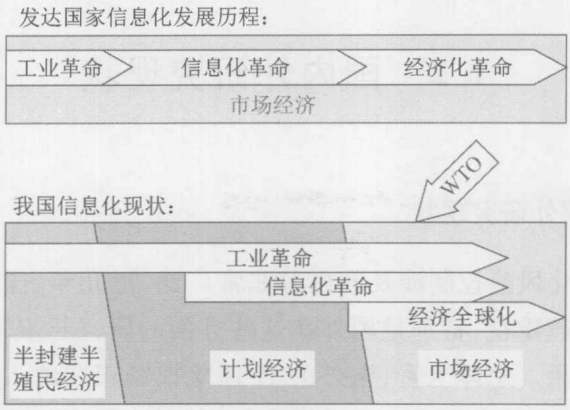

图 1-1 我国与发达国家信息化发展历程对比

资料来源：财政部企业司组编（付德一等）. 企业信息化管理[M]. 北京：经济科学出版社，2004(4)：37.

在这种背景下，我国企业往往没有经历西方企业的充分工业化阶段，而管理信息化过程又涉及企业生产、经营、技术和管理的各个方面，还涉及企业体制、市场环境等诸多因素，其复杂性可想而知。加之我国经济环境、企业管理体制的原因，我国企业管理中还有一些“人治”的色彩，比如，有许多地方是无章可循或有章不循；有的企业管理基础薄弱，不规范，工作方式因人而异等。比如，在标准化方面，我国绝大多数企业往往侧重于专业标准化而忽视事务性标准化。此外，我国很多集团公司往往由国有企业改制而来，公司治理结构还有待完善，并缺乏风险管理意识和机制。所以，对于我国集团公司而言，最迫切需要解决的是根据中国企业的实际情况，引进、消化、吸收西方先进的方法和经验，对管理信息化过程中所面临的各种风险及风险控制情况进行研究，这将有助于丰富和深化我国集团公司管理信息化风险控制的理论框架。

从实践上看，对我国集团公司当前在管理信息化风险控制的现状进行综合性调查研究，有利于发现、总结并分析目前我国集团公司管理信息化在风险控制方面存在的主要问题，并提出未来的改进途径与对策，以期为我国集团公司的管理信息化风险控制的实际工作提供一些参考。

因此，对于这一问题的研究，不仅在理论上，而且在实践上都具有重要的意义。这也正是本项研究的选题依据。

1.2 国内外研究现状

1.2.1 国外研究现状

管理信息化风险控制涉及的内容非常广泛，近几年，国内外对这些方面的研究越来越重视，特别是国外在这些方面的研究起步较早，且已经取得了丰硕的成果。总体上看，国外的IT风险控制正在纳入企业全面风险管理体系，并成为其中的一个交叉风险控制领域，管理信息化风险不再局限于常规的“操作风险”，它已成为企业的“经营风险”，未来企业的关注重点将逐渐扩展为战术层面、战略层面的风险，并把它们作为特定因素来管理，就笔者查阅的国外相关文献来看，国外研究现状可以从IT项目风险管理、IT服务及外包风险管理、IT信息安全管理、IT全面风险管理这四个方面来论述。

1. IT项目风险管理方面

近年来，国外关于IT项目风险方面的研究主要包括：Du，Keil，Mathiassen，Shen和Tiwana(2006)的研究，他们运用试验研究和假设验证的方法，对两组测试者(一组为102个具有高专业水平的IT项目管理专家，另一组为105个相对低专业水平的大学生)建立了一个风险识别模型，这个模型主要研究个人如何评估IT项目中的风险，以及什么影响了他们对于IT风险的认识。研究结果发现，对项目控制的意识状况会影响到个人对于项目中IT风险的认知。这可能向各组织表明，IT风险评估需要由组织内部的员工来执行，并且在IT项目评估中对他们进行适当控制，然后进行比较以期去除个人的风险认知偏见。[15] 此外，Johnstone，Huff和Hope(2006)研发了一个模型，来研究IT项目中的风险问题，特别是与项目相关的争端解决过程，并运用案例分析法验证了该模型的有用性，证实了该模型在评估项目冲突中是有效的。[35] Kliem(2004)提出了一个基于项目目标的风险及目标指标体系。[36]

2. IT服务及外包风险管理方面

Gewald和Helbig(2006)研发了一种治理模型来降低外包风险，这个模

型主要通过案例研究法总结而得出，它是建立在作为世界最大的外包服务商之一的公司所积累的丰富经验基础之上的，该模型由战略方向、治理原则和组织结构几部分组成。[18] Benvenuto 和 Brand（2005）识别了外包的驱动力，指出了风险分析过程，以及风险管理要素，并研发了一种通用的风险评估模型。[7] Bahli 和 Rivard（2005）对研发风险度量工具与外包 IT 运营相关的风险系数做出了贡献。他们研发出这些度量工具，并将这些度量工具运用于测试之前研究中已经识别出来的因素，以判断这些工具的可靠性，这些因素包括对 IT 外包风险有影响的交易风险、客户风险、供应商风险。最后论证了组织需要关注 IT 外包情形下的风险因素，以及项目风险评估能帮助决定执行哪一个外包项目。[5]

3. IT 信息安全管理方面

近年来，IT 信息安全风险集中了大量的研究，这些研究发现，对信息安全进行适当的管理对于组织来说是很重要的，并且，安全与业务连续性挂钩。这些研究同时还解释了为何信息安全过程不成功的原因，并实施了一些项目来评估组织 IT 安全过程的成熟度。

Ross（2006）探讨了信息安全与业务持续性管理之间的联系问题，发现安全与业务连续性挂钩，将业务持续性管理和安全作为风险管理范围内的两点，指出业务持续性管理是由物理事件导致的损失，而安全则是由逻辑事件导致的损失。并建议业务持续性计划应包括所有类型的中断而不仅仅只是灾难。[51] Pironti（2006）通过对 148 名 CISM（注册信息安全管理师）的调查，提出了一个对信息安全进行有效治理的过程，从研究中得到了 5 个基本成果，支持了正确有效的信息安全治理对组织是重要的这一观点。[47] Chapin 和 Akridge（2005）提出了一个评价组织信息安全规划成熟度模型，将风险评估过程与安全联系起来。[11]

Van Solms（2005）探讨了信息安全操作管理和信息安全合规管理之间的联系，定义并识别了信息安全治理这两个不同维度的关键组成部分。提出信息安全治理是好的整个 IT 治理和公司治理的组成部分，建议组织应设立独立的信息安全合规管理部门。[60] Stewart（2004）突出了关于信息安全风险评估的复杂性，指出了关于安全从业者、公司及安全行业在风险管理方面的新的方向。[56] Von Solms, B. & Von Solms, R.（2004）探讨了实施一个成功信息安全计划的相关问题，识别了公司在实施信息安全计划时的 10 个错误，提