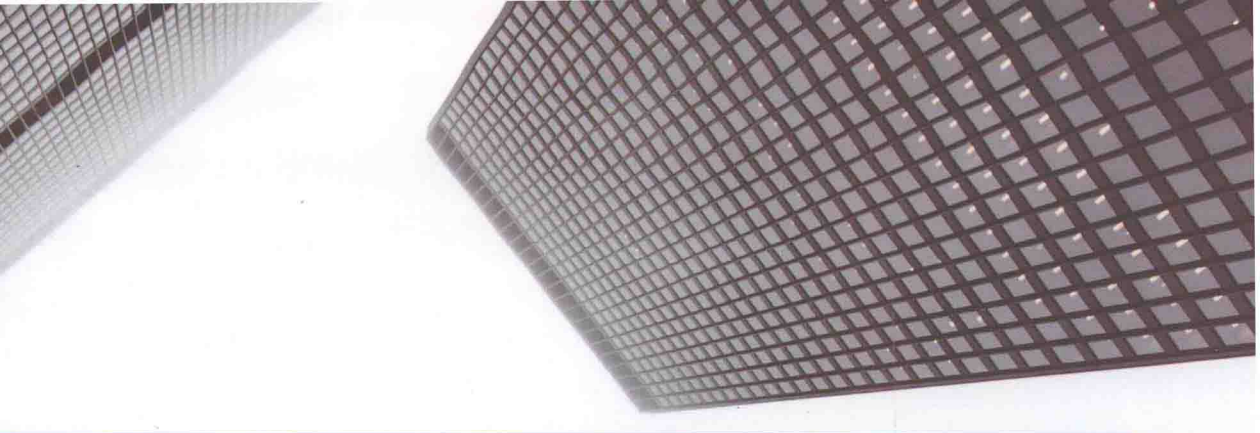


风险管理和内部控制理论与实践

RISK MANAGEMENT & INTERNAL CONTROL: THEORY AND PRACTICE

李　健◎编著

中国财经出版传媒集团
经济科学出版社
Economic Science Press

风险管理和内部控制理论与实践

RISK MANAGEMENT & INTERNAL CONTROL:
THEORY AND PRACTICE

李　健◎编著

中国财经出版传媒集团
经济科学出版社
Economic Science Press

图书在版编目（CIP）数据

风险管理和内部控制理论与实践/李健编著. —北京：经济科学出版社，2019.4

ISBN 978-7-5218-0485-0

Ⅰ.①风… Ⅱ.①李… Ⅲ.①企业内部管理-风险管理-研究-中国 Ⅳ.①F279.23

中国版本图书馆 CIP 数据核字（2019）第 077686 号

责任编辑：张 燕
责任校对：王肖楠
责任印制：邱 天

风险管理和内部控制理论与实践

李 健 编著

经济科学出版社出版、发行 新华书店经销

社址：北京市海淀区阜成路甲 28 号 邮编：100142

总编部电话：010-88191217 发行部电话：010-88191522

网址：www.esp.com.cn

电子邮件：esp@esp.com.cn

天猫网店：经济科学出版社旗舰店

网址：http://jjkxcbs.tmall.com

固安华明印业有限公司印装

710×1000 16 开 23.5 印张 480000 字

2019 年 5 月第 1 版 2019 年 5 月第 1 次印刷

ISBN 978-7-5218-0485-0 定价：78.00 元

（图书出现印装问题，本社负责调换。电话：010-88191510）

（版权所有 侵权必究 打击盗版 举报热线：010-88191661

QQ：2242791300 营销中心电话：010-88191537

电子邮箱：dbts@esp.com.cn）

序一

XUYI

奠稳风险管理和内部控制的基石，企业之舟才能扬帆远航

近年来，全球化和技术变迁正在不断改变着世界的政治格局和经济版图，企业面对的不确定因素不断增多，面对的风险也越来越复杂。波及全球的贸易战、金融危机以及时有发生的地区武装冲突、恐怖袭击、自然灾害、安全事故、环境污染等不仅给全球经济发展带来了巨大挑战，也直接威胁到企业的生存和发展。因此，企业开展风险管理和内部控制工作是顺应国际国内政治经济环境新变化的必然要求，也是现代企业实现健康稳定可持续发展的必要保障。

全球经济一体化的进程在很大程度上加剧了风险事件产生的影响，一个小的风险事件往往会打开一体化链条上的“潘多拉之盒”，形成多米诺骨牌效应，波及的方面和产生的连锁反应往往是很多国家和企业所始料未及的。这些都在客观上要求中国企业建立一套行之有效的风险管理和内部控制体系来抵御内外部的各种风险。

虽然中国企业经过了四十多年的发展，也经历了市场化和全球化的巨大考验，但中国企业的风险管理和内部控制工作依然处于初级发展阶段，与中国企业在全球化和世界经济中承担的角色还很不相称和匹配。未来企业开展风险管理和内部控制工作需要走出仅仅满足合规要求的禁锢，要“择高处立”，即这些工作要与企业整体战略密切结合，推动企业整体战略的实现，借此实现企业的盈利目标和增加企业价值。风险管理要帮助企业管理者进行战略分析和提供决策选项，确保企业战略得到有效的执行。而内部控制是企业通过内部管控措施有效应对风险的重要手段，是企业综合能力的体现，也是企业竞争力的重要来源。

毫无疑问，以上这些变化和挑战要求企业管理者和学者从战略和创新发展的角度来审视风险管理和内部控制，并将两者与企业的整体战略、企业日常经营管理和业务流程

密切融合，以便应对企业发展进程中不断出现的新的挑战。

本书的作者李健博士是我最优秀的博士生之一，具有很强的研究创新能力、严谨的治学态度和极强的进取精神，善于通过跨学科研究和理论与实践相结合的方式实现学术上的突破。在《风险管理和内部控制理论与实践》的编写过程中，他融入了自己在世界五百强企业从事风险管理和内部控制工作多年积累的经验，结合理论研究的最新成果和行业内的最佳实践，阐述了风险管理和内部控制等各个方面，是一部不可多得的学术新作。该书有助于读者掌握风险管理和内部控制的游戏规则，了解企业开展风险内控工作的具体方法，提高风险管理和内部控制的理论和实践水平。

金占明
清华大学创新创业与战略系
教授　博士生导师

序 二

XUER

近十多年来，放眼全球，人们看到了大洋彼岸许多不良的公司治理和内部控制失效的事件，由此而引发的一系列的财务丑闻和舞弊案件以及国际金融危机，对企业和社会经济发展产生了巨大的破坏性影响。社会各界人士的口诛笔伐，促使美国监管部门出台了《萨班斯—奥克斯利法案》等一系列的法律法规和标准，要求上市公司加强内部控制和完善公司治理。

现代内部控制是一种综合管理体系，包含着经营管理的精髓、理念和控制措施，是企业运营和各项管理工作的基础；企业风险管理强调治理和文化的上层建筑，支持企业使命、愿景和核心价值的实现。按照美国反虚假财务报告委员会下属的发起人委员会（COSO）在2017年版企业风险管理整合框架中的最新解释，内部控制主要聚焦在企业的运营和对于相关法律法规的遵从性上，例如，企业需要关注与财务报告目标相关的舞弊风险、与合规目标相关的控制活动、与运营目标相关的持续及独立评估。风险管理则包括了管理风险的文化、能力和实践，更加强调风险与价值的相结合，突出价值创造而不只是防止损失。COSO一再强调，风险管理和内部控制两个框架是截然不同的，并提供不同的重点；它们不可相互取代，而是互补的关系。二者是公司治理不可缺少的两个组成部分。

在企业内部控制规范体系建设方面，我国政府监管部门充分利用了后发优势，在借鉴和吸收国际监管新理念，通过整合资源与合力攻坚，2008年5月和2010年4月，我国财政部、证监会、审计署、银监会和保监会五部委联合制定和先后发布了《企业内部控制基本规范》和《企业内部控制配套指引》，构建了中国企业内部控制规范体系。近10年来，这场由我国政府监管机构主导的旨在加强企业内部控制体系建设的系统工程，大约可分为三个阶段。

第一阶段（2008～2011年），开展普及内控规范体系和相关知识的培训教育运动。尽管从总体上说，这种以搞运动的方式开展内控培训，是否真正达到了“人人学内控、人人讲内控、个个受约束”的效果还有待实践检验，但对于自上而下层层传导式地推进企业内控规范体系的实施起了促进作用，这一点是毋庸置疑的。

第二阶段（2012～2016年），以内控评价促进企业内控体系建设。由于一些企业，尤其是上市公司自我约束的内在动力不足，企业内部控制规范体系中专门规定了“施行企业内部控制规范体系的企业，必须对本企业内部控制的有效性进行自我评价，披露年度自我评价报告”要求，同时还要求企业“聘请会计师事务所对其财务报告内部控制的有效性进行审计，出具审计报告”。政府监管部门强化对企业内部控制规范体系实施情况的检查与考核，这种“以评促建”的方式，无疑对上市公司建立内部控制体系发挥了强制性的推动作用。

值得一提的是，2012年5月7日，国资委和财政部联合发布了《关于加快构建央企内控体系有关事项的通知》。通知要求，各中央企业要力争用两年时间，按照《企业内部控制基本规范》和配套指引的要求，建立规范、完善的内部控制体系。央企和地方国企由此拉开了建立和实施内部控制体系的大幕。

第三阶段（2017年至今），企业建设内部控制体系由外部推动变为内在需求。当前，国内外环境正发生深刻变化，企业发展亦面临诸多不确定因素，我国监管机构积极寻求规避风险和化解矛盾的应对举措。从金融去杠杆的推进，到强化银行同业、资本市场、保险业务的监管；从国有企业完成公司制改制，加强企业海外经营合规管理，再到财政部印发《小企业内部控制规范（试行）》，层出不穷的监管要求，对企业进一步完善风险管理和内部控制体系施加了倒逼压力。企业内部控制体系建设由点带面，由浅入深，从原先的“要我控制”变成了“我要控制”，从单纯的制度建设转向追求内控制度的实际操作及其有效性。治理层和高级管理层更加关注如何实现战略目标和提升经营绩效，在消除各行业风险隐患的基础上，加强薄弱环节监管制度建设，确保企业依法合规经营，完善风险控制机制，找到企业变革和创新转型的抓手，实现持续改进和提升价值。

李健博士一直负责中国化工集团的风险管理和内部控制工作。近10年来，他全过程参与了其所在集团从风险控制体系建设，风险识别和评估、试点及推广项目，到全体系的内部控制评价检查工作，积累了丰富的实践经验，并具备了较全面的综合管理和协调能力。本书是李健博士近10年来在中国化工集团从事风险管理和内部控制工作的实践经验总结。作者结合国资委对中央企业全面风险管理的各项要求和财政部等五部委对企业贯彻落实内部控制规范体系的指引和规定，从风险管理和内部控制概述，风险内控体系建设，风险的识别、评估和应对，公司层面和业务层面控制，内部控制评价，风险内控信息化六个方面，详细论述了风险管理和内部控制从规划、实施、评价检查，以及整改和信息化的各个环节的重点内容，面临的主要风险和相应的控制措施，力图为企业开展风险管理和内部控制工作提供有效的指导。

企业建立和实施内部控制是一项专业性很强的工作，要求相关人员具备丰富的知识技能和充足的实践经验。为了解决目前普遍存在的制度建设与实际操作“两张皮”的现象，企业需要把内部控制的有效执行放在首位。在开展内控体系建设的过程中，一些

企业由于缺乏内控专业人才，或相关工作人员缺乏相应的知识和经验，从而影响企业内部控制体系建设的质量和持续改进。本书的出版发行不仅为我国上市公司和国有企业的内部控制体系建设提供可供选择的实务操作指南和解决方案，而且可作为内部控制培训项目的适用辅导教材，有利于培养风险内控专业人才，促进企业内部控制体系建设紧密结合自身实际，实现控制目标和提升经营管理绩效。

张　玉

中国大陆首位高级国际注册内部控制师

中国职协企业内控师岗位培训项目资深顾问

2019 年 5 月

前言

QIANYAN

人类社会的存在和发展自始至终都伴随着风险，识别、评价和应对风险是人类的本能，也是人类得以生存繁衍的基础。随着社会的进步，人类的风险意识和应对能力也在不断提高。同样的，企业在生存和发展过程中也会遇到各种各样的风险，会对企业整体经营目标的实现产生影响，这些风险可能来自企业所处的外部环境也可能来自企业的内部。

风险管理就是帮助企业在发展业务的同时，对危及目标实现的可能性提前预判，并采取有效的措施加以预防。而内部控制是风险管理的重要手段，企业通过将内部控制的要求融入各项业务管理过程中，对企业制度和流程进行规范和监督评价，实现管控“内力”的提升。风险管理和内部控制能够保证企业健康、稳定和可持续发展，为企业战略目标的实现保驾护航。

不仅如此，风险管理作为企业整体战略的重要组成部分，它还能帮助企业在错综复杂的环境中识别危机和机遇，结合自身的资源和能力，抓住机遇实现更快的发展，促进企业战略目标的实现，提升企业的价值。这既是企业满足外部合规要求的需要，也是企业提高经营效率和效益的关键。

中国改革开放四十年来，很多企业规模迅速扩大，企业效益明显增长。但中国企业在发展过程中也遇到很多机遇和挑战，突出表现在国内外各方面监管要求越来越严格，违规处罚的力度越来越大，而企业整体的风险管理和内部控制水平无法跟上规模扩大和国际化的步伐，各类风险事件频出。

目前，很多国内企业的风险内控工作还处于满足合规要求阶段，距离实现风险量化、实时监控、及时预警和为管理层提供决策支持等方面还有很大的差距。未来，中国企业需要进一步推动风险内控工作的开展，走出合规要求和规范管理的限定，有效化解风险和危机，推动企业的持续创新和自我优化提升，更好服务于企业整体战略和价值创造的目标。

基于这种考虑，本书解读了风险内控最新理论和合规性要求，系统介绍了从整体规划到实际执行，从评价检查到完成整改和提升，以及实现信息化管理的整个风险内控工

作过程，以期为企业开展风险内控工作提供有效的指导。

本书的理论部分系统阐释了风险管理和内部控制的概念、理论演进过程、对企业的重要意义等，对风险管理、内部控制、审计、合规管理等概念进行了界定；对国内外风险内控的最新规定，比如2017年版风险管理框架等予以解读；探索和分析了中国企业风险内控工作的现状和存在的问题，并对我国企业风险内控工作的未来发展提出了一些设想。

实践部分结合作者的实际工作经验，以案例的形式分析了国内外一些企业开展风险内控工作的最佳实践和经验教训，提出开展风险内控工作的方式和方法，包括风险内控总体规划、风险识别和量化评估、内部控制组织和制度体系建设、公司层面（组织、战略、人力资源等5类）和业务层面（采购、生产、销售、资金等13类）的主要风险及内部控制措施、内部控制评价方法（抽样和测试方式等）、内控缺陷认定标准、风险监控和预警、内控成熟度评价，以及企业风险内控信息化建设等。

与以往风险内控类的书籍有所不同，本书的创新点在于：将风险内控工作与企业战略有机结合，系统诠释风险管理在企业战略制定和执行中发挥的作用；对最新风险内控合规要求进行详细解读；本书涵盖了风险内控最前沿的研究领域，包括风险量化评估、关键风险指标体系设计、风险监控和预警体系搭建、内部控制成熟度评价、风控信息化等相关内容。在国内已出版发行的书刊中，相关内容鲜有涉猎，本书顺应企业界的实际需求在以上方面做出了有益的探讨和尝试。

本书由李健编著，同时获得了德勤、信永中和等咨询机构、国际内部控制协会等机构及众多企业管理人员的支持，为本书编写提供支持和帮助的还有况成功、张赵坤、胡宇、陈蔚然、李慧、周洁、谢冰、庞云等，作者对上述机构和人员所付出的努力表示衷心感谢。

由于风险内控工作所涉及的业务领域较为宽泛且深入，风险内控工作因企业、行业的实际情况而具有较大差异，书中存在的不足之处，恳请各位读者提出宝贵的意见和建议。

作者邮箱：lij.05@sem.tsinghua.edu.cn。

作者

2019年4月

目 录

MULU

第一章 风险管理和内部控制概述 …… 1

第一节 风险和风险管理 …… 1

一、风险的概念 …… 1

二、风险的分类 …… 2

三、风险管理理论的演进 …… 7

四、2017 年版企业风险管理框架 …… 12

第二节 内部控制 …… 17

一、内部控制的概念 …… 17

二、内部控制的重要性 …… 22

三、内部控制的基本原则 …… 23

四、内部控制发展历程 …… 25

五、2013 年版内部控制框架 …… 30

六、内部控制局限性 …… 35

第三节 风险管理、内部控制与合规管理 …… 38

一、风险管理和内部控制的关系 …… 38

二、风险管理、内部控制与合规管理的关系 …… 40

三、风险管理、内部控制与内部审计的关系 …… 46

四、风险管理、内部控制与业务的关系 …… 48

第四节 风险管理和内部控制相关法规 …… 50

一、安然事件 …… 50

二、《萨班斯—奥克斯利法案》简介 …… 51

三、我国风险管理和内部控制规范的演进 …… 54

四、《中央企业全面风险管理指引》主要内容 …… 57

五、《企业内部控制基本规范》主要内容 …… 64

六、《企业内部控制基本规范》应用指引主要内容 …… 66
第五节 中国企业风险内控的现状和未来 …… 70
一、中国企业内部控制现状 …… 70
二、中国企业风险内控工作中存在的问题 …… 71
三、中国企业风险内控的未来发展 …… 74

第二章 风险内控体系建设 …… 77

第一节 总体规划 …… 77
一、前期分析调研 …… 77
二、主要工作难点分析 …… 79
三、实施原则 …… 81
四、启动会 …… 82
第二节 组织架构搭建 …… 83
一、组织架构概述 …… 83
二、风险内控组织架构 …… 84
三、风险内控部门职责 …… 88
四、对企业风险内控部门定位的思考 …… 89
第三节 制度体系建设 …… 91
一、制度的概述 …… 91
二、风险内控制度体系构成 …… 94
三、制度管理 …… 95
第四节 风险内控手册编制 …… 102
一、风险管理手册和内部控制手册概述 …… 102
二、集团型企业内部控制手册类型 …… 105
三、内部控制手册的展现形式 …… 106

第三章 风险的识别、评估和应对 …… 117

第一节 风险识别 …… 120
一、风险识别的概念 …… 121
二、风险识别的程序 …… 125
第二节 风险评估 …… 130
一、根本原因分析 …… 132
二、风险发生的可能性 …… 134
三、风险影响程度 …… 136

四、风险评级 …… 138
五、风险热力图 …… 140
第三节　风险应对 …… 142
一、风险偏好和风险承受度 …… 143
二、风险应对策略 …… 144
三、风险应对有效性评估 …… 148
四、风险与创新 …… 149
第四节　风险预警和关键风险指标 …… 151
一、风险监控和风险预警概述 …… 151
二、风险预警体系的建立 …… 153
三、关键风险指标体系概述 …… 154
四、关键风险指标体系建设路径 …… 156
五、关键风险指标体系的拓展应用 …… 161

第四章　公司层面控制 …… 164

第一节　组织架构的内部控制 …… 164
一、治理结构和内部机构 …… 164
二、组织架构的责权分配 …… 165
三、组织架构的内部控制 …… 167
第二节　企业战略的内部控制 …… 169
一、战略的概述 …… 169
二、战略管理的理论研究 …… 171
三、战略管理的内部控制 …… 181
第三节　人力资源的内部控制 …… 184
一、人力资源的引进与开发 …… 185
二、人力资源的约束与激励 …… 187
三、薪酬福利管理 …… 188
四、人力资源的使用与退出 …… 189
五、员工档案管理 …… 190
第四节　社会责任的内部控制 …… 193
一、安全生产 …… 193
二、质量管理 …… 197
三、节能环保 …… 198
四、促进就业与员工权益保护 …… 199

第五节　企业文化的内部控制 …… 200

第五章　业务层面控制 …… 203

第一节　资金管理的内部控制 …… 203
一、筹资 …… 204
二、资金营运 …… 205
三、金融衍生业务 …… 209
四、担保业务 …… 211
第二节　投资管理的内部控制 …… 215
一、投资方案与决策 …… 215
二、投资执行 …… 216
三、投资企业管理 …… 218
四、投资后评价 …… 221
第三节　采购业务的内部控制 …… 223
一、采购计划 …… 225
二、供应商管理 …… 227
三、采购执行与验收 …… 230
四、采购付款 …… 234
五、业务外包 …… 237
第四节　生产管理的内部控制 …… 240
一、生产计划 …… 240
二、生产运行 …… 241
三、生产监督 …… 242
四、生产成本 …… 242
第五节　存货管理的内部控制 …… 245
一、入库管理 …… 245
二、库存管理 …… 246
三、出库管理 …… 247
四、存货处置 …… 248
五、物流运输 …… 248
第六节　销售业务的内部控制 …… 250
一、销售计划 …… 250
二、客户管理 …… 253
三、销售定价 …… 254

四、销售渠道管理 …… 255
五、收款管理 …… 256
六、客户服务 …… 258
第七节　研究与开发的内部控制 …… 260
一、立项与研发计划 …… 260
二、技术及产品应用 …… 262
三、知识产权保护 …… 263
第八节　工程项目的内部控制 …… 264
一、工程立项 …… 264
二、工程招标 …… 265
三、工程建设 …… 268
四、工程验收与竣工决算 …… 272
第九节　资产管理的内部控制 …… 275
一、固定资产管理 …… 275
二、在建工程 …… 277
三、无形资产管理 …… 278
第十节　财务管理的内部控制 …… 279
一、全面预算 …… 279
二、税务管理 …… 284
三、会计核算 …… 286
四、财务报告 …… 287
五、成本与费用管理 …… 289
六、关联交易 …… 290
第十一节　法律事务的内部控制 …… 292
一、合同管理 …… 292
二、纠纷与诉讼管理 …… 295
第十二节　信息系统的内部控制 …… 298
一、信息系统规划 …… 299
二、信息系统开发 …… 299
三、信息系统运行维护 …… 300
四、信息安全 …… 302
第十三节　综合管理 …… 303
一、综合办公 …… 303
二、制度管理 …… 306

三、信息传递 …… 306
四、保密管理 …… 308

第六章 内部控制评价 …… 310

第一节 内部控制评价概述 …… 310
一、内部控制评价的目标 …… 311
二、内部控制评价的主体 …… 311
三、内部控制评价的范围 …… 312
第二节 内部控制评价程序和方法 …… 314
一、内部控制评价程序 …… 315
二、内部控制评价方法 …… 317
三、内部控制评价检查内容 …… 326
四、内部控制缺陷认定 …… 333
五、内部控制评价工作底稿 …… 337
六、内部控制成熟度评价 …… 339

第七章 风险内控的信息化 …… 345

第一节 风控信息化的重要性 …… 345
一、风控信息化的内在需求 …… 346
二、外部监管要求 …… 347
第二节 风控信息化建设 …… 348
一、风控信息化应注意的问题 …… 348
二、风控信息化平台建设的目标 …… 349
三、风控信息化的基础和前提 …… 350
四、风控信息化的具体内容 …… 352
第三节 风险内控应用软件 …… 353
一、风控信息化软件应用现状 …… 353
二、国内企业风险内控信息化现状 …… 355
三、SAP GRC 系统功能和模块介绍 …… 356

参考文献 …… 361

第一章　风险管理和内部控制概述

第一节　风险和风险管理

自人类诞生之日起风险就一直相伴，可以说人类对风险的认知与人类的历史一样悠久。在挑战自然、挑战自身极限的过程中人类都曾付出巨大的代价。1986 年和 2003 年“挑战者”号和“哥伦比亚”号航天飞机的失事，共导致 14 名宇航员遇难。1912 年号称“永不沉没的巨轮”泰坦尼克号处女航时就撞到冰山而沉没，超过 1500 人在事故中遇难。人类为自己的过度自信和冒险行为付出了沉重的代价，但也正是这种无畏和勇于探险的精神一直鼓舞和激励着人们去探索未知的世界，才有了今天繁荣发达的人类社会。现如今，风险（risk）一词在我们生活中出现的频率越来越高，在电视、电影、广告、报纸、杂志上都能听到和看到风险的字眼，上到人类整体的未来，全球自然环境、政治经济环境等，下到企业和个人的发展，在遇到不确定性、面对困难和挑战时人们都会把风险一词挂在嘴边。

在市场经济环境下，企业为了生存和发展，必须承担必要的风险，追逐更高的利润，同时避免出现过高的风险而导致企业遭受损失。对企业来说，每一次投资和并购，每一次做出重要的决策都是打开一扇未知的门，永远不知道门后到底是美女还是老虎。而风险管理所能做的就是把打开门后见到老虎的概率降到最低，并采取有效的风险防范措施，避免在没有做出认真分析评估，没有采取有效应对措施的情况下就打开那扇门。

一、风险的概念

对于风险的定义，最为人们普遍接受的是 1921 年美国经济学家佛兰克·奈特在他的《风险，不确定性和利润》一书中提出的：风险是可测定的不确定性。2004 年美国反虚假财务报告委员会下属的发起人委员会（以下简称 COSO 委员会）将风险定义为：某个事件即将发生并给目标实现带来负面影响的可能性；2017 年在新版的企业风险管