



华南理工大学

South China University of Technology

专业学位硕士学位论文

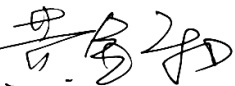
F 公司软件项目风险管理研究

作者姓名	黄金和
学位类别	工商管理
指导教师	万江平 教授
所在学院	工商管理学院
论文提交日期	2013-6-20

华南理工大学

学位论文原创性声明

本人郑重声明：所呈交的论文是本人在导师的指导下独立进行研究所取得的研究成果。除了文中特别加以标注引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写的成果作品。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律后果由本人承担。

作者签名： 日期：2013年6月21日

学位论文版权使用授权书


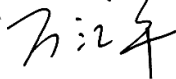
本学位论文作者完全了解学校有关保留、使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属华南理工大学。学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许学位论文被查阅（除在保密期内的保密论文外）；学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存、汇编学位论文。本人电子文档的内容和纸质论文的内容相一致。

本学位论文属于：

☐ 保密，在____年解密后适用本授权书。

☒ 不保密，同意在校园网上发布，供校内师生和与学校有共享协议的单位浏览；同意将本人学位论文提交中国学术期刊(光盘版)电子杂志社全文出版和编入 CNKI《中国知识资源总库》，传播学位论文的全部或部分内容。

(请在以上相应方框内打“√”)

作者签名： 日期：2013.6.21
指导教师签名： 日期：2013.6.21
作者联系电话： 电子邮箱：
联系地址(含邮编)：

A Research on Risk Management for Software Project of F Company

A Dissertation Submitted for the Degree of Master

Candidate: Huang Jinhe

Supervisor: Prof. Wan Jiang Ping

South China University of Technology
Guangzhou, China

分类号：C93

学校代号：10561

学 号：201021535834

华南理工大学硕士学位论文

F 公司软件项目风险管理研究

作者姓名：黄金和

指导教师姓名、职称：万江平 教授

申请学位级别：硕士

学科专业名称：工商管理

研究方向：企业管理

论文提交日期：2013 年 6 月 20 日

论文答辩日期：2013 年 5 月 17 日

学位授予单位：华南理工大学

学位授予日期：2013 年 6 月 日

答辩委员会成员：

主席： 李志宏

委员： 李锋 徐咏梅

摘 要

IT 系统建设普遍具有投入高、业务影响广、安全要求高等特点，系统建设的不确定因素比较多，具有很强的风险性，加强软件项目的风险管理，对于提高软件系统建设的成功率具有重要意义。

本文结合 F 公司软件项目实施，对 F 公司软件项目的风险管理进行了研究与分析，构建了 F 公司软件项目全面风险管理体系，体系由八个相互关联的模块组成，分别是风险管理环境，风险管理目标与政策设定，风险监测与识别，风险评估，风险定价与处置，内部控制，风险信息处理和报告，风险持续改进。

基于 F 公司软件项目实施过程中存在的风险因素，通过问卷调查研究了 F 公司软件项目实施中的关键风险因素。研究表明：需求分析不准确、供应商选择失误、需求变更风险、外包决策风险、缺少用户支持、里程碑失控、设计方案出现偏差、沟通风险、人力资源风险、进度风险等十大风险是影响 F 公司软件项目实施的关键风险因素。

针对 F 公司软件项目实施的关键风险因素，运用解释结构模型（ISM）的方法研究了 F 公司软件项目实施的风险因素关系，研究表明风险的根源由一个具有四级递阶的层次结构的因素梯级组成。其中人力资源风险、供应商选择失误、沟通风险处在最底层，是导致项目实施失败根源原因。

本文采用风险管理理论和具体实践对 IT 项目风险管理进行了系统的分析和研究，研究结果如下：（1）在 F 公司 IT 项目风险管理分析的基础上，构建了 F 公司软件项目全面风险管理体系。（2）以 F 公司软件项目为例，应用 ISM 解释结构模型分析得出 F 公司软件项目的风险解释结构模型。（3）对 F 公司 IT 项目面临的项目关键风险进行了分析和描述，并提出了具体的规避措施。

总之，本文应用解释结构模型分析 F 公司在软件项目过程中所存在的各种风险因素之间的关系以及风险产生的根源，并提出了相应的风险管理解决方案和实施方法，其目的就是改进 F 公司 IT 项目风险管理能力，从而对项目风险进行有效控制。

关键词 项目管理；风险管理；生命周期；全面风险管理；解释结构模型

ABSTRACT

With the continuous progress of the development of information technology, the daily work is increasingly dependent on IT system. IT systems generally have high investment, big impact on business, high security requirements. So IT system has more and more the uncertainties factor and has a strong risk. It's very important significance that we strengthen risk management of software projects to improve the success ratio of software systems.

In this context, combine with the implementation of F company software project, risk management theory is applied to the actual software project, this paper provide a set of scientific, complete, practical guide for software project risk management tools, to ensure the normal running smoothly, system project and support business smoothly. This paper is devoted to the risk and control strategy of F Company IT project research, including the important questions in this thesis. First what kind of risks of the software project in finance company? Second, what kinds of actions should finance company take? Third, is there a Risk Management Model for them to enhance their risk monitoring and control level? Last, How to avoid all kinds of project risk in order to ensure the project progress?

On the base of the studies of risk management development, lifecycle management, and the practical of many experts throughout the world, and the case study of software project from F company, three results are put forward: (1) Excogitate out a risk management model according to projects of communications industry. (2) By using Interpretive Structure Model, the risk structure of BI project is issued. (3) The descriptions and solutions of key risks for communications projects are expounded in detail.

In brief, in the process of risk management study, interpretive structure model(ISM) helped finance company build the structure of relationship between risks. Based on the theories and studies of risk management, some practical suggestions will help F Company to build a suitable risk management system.

Keywords: Project; Project Management; Risk Management; Lifecycle; Wide risk Management; Financial Industry; Interpretive Structure Model

目 录

摘 要.....	I
ABSTRACT.....	II
图表清单.....	VI
第一章 绪论.....	1
1.1 选题背景及意义.....	1
1.2 风险管理理论文献综述.....	3
1.2.1 项目风险管理发展概况.....	3
1.2.2 IT 项目全生命周期.....	4
1.2.3 全面风险管理体系.....	4
1.2.4 经典风险管理理论.....	7
1.3 研究内容与方法.....	10
1.4 论文结构和创新点.....	11
第二章 项目风险管理模型.....	13
2.1 软件项目风险特点.....	13
2.2 全面风险管理理论.....	14
2.2.1 项目全面风险管理.....	15
2.2.2 项目全生命周期风险管理.....	15
2.3 风险管理过程.....	17
2.3.1 编制风险管理计划.....	18
2.3.2 风险识别.....	18
2.3.3 风险分析.....	21
2.3.4 风险应对.....	22
2.3.5 风险跟踪.....	24
2.3.6 风险控制.....	25
2.3.7 风险数据库.....	26
2.4 本章小结.....	26
第三章 F 公司软件风险管理.....	27

3.0 F 公司及项目概况	27
3.1 构建全面风险管理体系	28
3.2 风险管理体系建设	31
3.3 项目风险管理计划	32
3.4 项目风险识别过程	34
3.5 项目风险控制策略	37
3.6 本章小结	38
第四章 基于 ISM 模型的风险分析	39
4.1 项目主要风险	39
4.2 项目全过程风险识别	40
4.3 建立构思模型	41
4.4 建立重排序的可达矩阵	44
4.5 建立解释结构模型	45
4.6 解释结构模型分析	45
4.7 对项目风险管理的一些建议	46
4.8 本章小结	47
第五章 F 公司软件项目关键风险规避与对策	48
5.1 需求分析风险	48
5.1.1 风险描述	48
5.1.2 规避措施	49
5.2 项目沟通风险	50
5.2.1 风险描述	50
5.2.2 规避措施	51
5.3 项目进度风险	51
5.3.1 风险描述	51
5.3.2 规避措施	52
5.4 设计方案风险	53
5.4.1 风险描述	53
5.4.2 规避措施	54

5.5 项目合作风险	54
5.5.1 风险描述	54
5.5.2 规避措施	55
5.6 本章小结	56
结 论	57
参考文献	59
附 录	62
攻读硕士学位期间取得的科研成果	67
致 谢	68

图表清单

图 1-1 项目全生命周期基本框架.....	4
图 1-2 全面风险管理体系	5
图 1-3 研究框架	11
图 2-1 全生命周期风险管理体系框架	16
图 2-2 全生命周期项目风险管理过程	18
图 2-3 风险识别过程定义	19
图 2-4 风险分析过程	21
图 2-5 风险计划过程定义	22
图 2-6 风险跟踪过程定义	24
图 2-7 风险控制过程	25
图 3-1 F 公司项目特点.....	28
图 3-2 全面风险管理体系	29
图 3-3 F 公司信息科技风险管理体系结构图.....	31
图 3-4 全生命周期风险识别过程	35
表 3-1 软件项目生命周期各阶段主要风险与次要风险表	36
表 4-1 金融机构 IT 项目风险列表	39
表 4-2 项目风险因素清单	41
表 4-3 调查结果表	42
图 4-1 邻接矩阵	42
图 4-2 可达矩阵	43
图 4-3 骨架矩阵	43
图 4-4 重排序的可达矩阵	44
图 4-5 风险结构模型	44
图 4-6 解释结构模型	45
图 5-1 项目状态板	53

第一章 绪论

介绍本文的选题背景和研究的意义，总结目前项目风险管理研究发展的概况和国内外先进的项目风险管理理论，在分析 IT 项目生命周期和全面风险管理体系理论的基础上，提出本文研究内容和采用的方法。

1.1 选题背景及意义

1.1.1 选题背景

当前，金融创新已成为中小金融机构的核心竞争力，其中 95% 的金融业务创新的实现，都非常依赖于信息技术。另外，金融管理决策正向智能化方向逐渐发展，由信息科学技术构建的金融工具，能够实时对金融风险进行识别、分析、度量和控制，提高了金融管理决策的效率。并且信息技术还使得比较复杂的金融产品交易成为现实。因此，金融信息化正成为中小金融公司面临重要的研究课题，该课题需要从更广阔的角度研究中国金融体制变革和中国金融信息化的总体发展战略布局，实现金融信息化系统的整合，全方位提升中小金融公司金融竞争力，并且金融信息化也是促进金融行业快速发展和国民经济快速持续发展的需要。

由于金融业对信息科技的高度依赖，使得信息技术系统的安全性、可靠性和有效性直接影响到整个银行业的安全和金融体系的稳定。自 2010 年以来，监管部门对信息科技风险管理高度重视，先后颁布了《商业银行科技风险管理指引》，《商业银行数据中心监管指引》，《商业银行业务连续行监管指引》等指引和规范性文件，并于 2011 年成立了银行业信息科技风险管理高层指导委员会，以全面风险管理为导向，以推动金融行业信息科技持续，健康发展为宗旨。由各金融机构投入大量人力加强信息安全体系建设，防范各种信息科技风险。

汽车金融公司作为非银行业金融机构，向流通环节的汽车经销商提供采购融资支持，以及为终端机构客户和个人购车者提供购车贷款业务等专业化金融服务。其贷款业务量逐年攀升，为了支持业务的快速发展，大量的信息系统投入建设，系统之间以及项目之间需要有效配合。也就要求各个系统之间不能出现偏差，这给 IT 系统的建设和运营管理带来巨大的压力。如果在系统建设过程中管理控制能力不能及时跟上，势必降低软件产品质量，进而引发系统运行风险。在这种情况下，金融 IT 项目的风险管理就显得格外重要。如何识别、分析风险并采取应对策略，对项目的成功实施至关重要。

本文着重从三方面入手：一、在项目计划阶段要尽早进行风险规划，及早识别项

目风险,对识别出来的风险进行定性分析,采用适当的方法进行定量分析,并根据风险的结果,并结合项目实际情况制定具体的风险应对策略;二、在整个项目执行阶段都需要对项目进行风险监控,关注风险变化情况随时采取适当的风险应对策略;三、项目收尾阶段,项目组需要对项目风险进行总结分析,以丰富公司的风险数据库和组织过程资产^[1]。全面化的、精细化风险管理既是项目经理(PM)的重要职责,也是项目全体成员共同参与的过程。

2.选题意义

软件项目风险管理就是对影响软件项目、实施过程或系统使用的风险进行评估和控制的实践过程。当前软件行业非常重视项目风险管理,从理论上对软件项目风险进行了分类,提出了项目风险管理的思路,在实践上也已经有定量管理风险的方法和项目风险管理的信息系统。然而,随着业务需求和计算机硬件资源的不断提升,软件系统的规模越来越大,复杂程度越来越高,并且项目周期越来越短、项目任务多、核心技术开发人员稀缺等等问题,都会给软件项目实施带来各种风险,项目实施成果不能满足业务的要求,项目成本超支、计划拖延厉害的现象非常普遍,对软件项目的这些灾难,进行事后调查分析发现,如果这些公司提前进行风险因素识别,并规避高风险因素,在项目实施过程中不断管理风险,这些因素是可以避免或减少其对项目的影响。因此,用户和 IT 部门都非常关心哪些因素导致软件项目的失败?这些因素对项目的影响有多大?怎样控制这些因素?这些问题都是软件项目风险管理问题。因此,本文研究 IT 项目的风险管理,将起到以下的积极作用:

(1) 项目顺利完成的重要保障。由于金融公司各种信贷业务非常复杂,业务需求多种多样,风险管理稍有失误很可能导致整个 IT 项目失败,进而影响公司业务的开展,甚至失去业务部门对 IT 系统的信赖。

(2) 将理论与实践相结合,从信息化战略管理的角度来系统研究与企业信息化项目管理相配的风险管理模式,并建立相关的模型与框架,是对现有理论、企业生存与发展理论的一种深化。

(3) 对企业未来的发展影响深远。没有好的全面风险管理的实施方法和战略,再优秀的理论也只能在书本上存在,对企业没有任何实际的意义。通过好的实施方法和战略,尽快建立起完善的风险防范措施,是企业建立完善风险制度,规避项目风险,使项目顺利开展的重要保障。

1.2 风险管理理论文献综述

1.2.1 项目风险管理发展概况

项目风险管理是在企业风险管理理论和金融风险管理的理论以及实践基础上产生的。项目风险管理出现比较晚,随着项目管理发展,特别是大型建设工程项目或科研技术项目的开展与管理需要,风险管理才被逐步引入项目管理理论和实践中,并形成了项目风险管理。

现代项目管理起源于 20 世纪 70 年代。在此之前,项目管理主要包括项目范围、资金、时间、质量和采购等等方面的内容,项目管理的对象主要是“创造独特产品或服务”。进入 80 年代,各种项目日益繁多,项目规模日益扩大的趋势,项目外部环境难以把握,项目成功正面临越来越多的风险考验。与此同时,项目人力资源、项目沟通等问题,在项目的风险管理领域开始受到关注。同时,项目风险管理也逐渐成为各大企业、政府部门等的经常性事务工作;并且计算机技术的发展也极大地促进了项目管理的发展^[2]。

项目管理的普及需要规范的项目管理学科体系作为理论基础,于是世界各国的项目管理组织纷纷建立立足于本国的项目管理知识体系,在各国的项目管理知识体系中基本都把风险管理作为重要的管理内容之一^[3]。1986 年,项目风险管理作为一个相对独立的管理学科,被美国项目管理学会委员会(PMI)纳入有关项目管理知识体系。非常具有影响力的国际项目管理协会(IPMA, International Project Management Association)在每两年召开一次的年会上对项目风险管理进行研讨,进一步理清了风险管理的理论研究。于 1992 年 6 月在意大利召开的第 11 届大会上,将项目风险管理单独列为一个主题,并出版了论文集《Project Management Without Boundaries》,其中有关项目风险相关的文章约占 10%。在两年后的挪威奥斯陆召开的第 12 届学术年会上,再次将项目风险管理作为本次大会的主题之一^[6]。美国项目管理协会(PMI)在项目管理体系(PMBOK)中把项目管理划分为 9 个知识领域,把项目风险管理作为其中的一个单独知识领域。在其 2004 版项目管理知识体系(PMBOK)中,把风险管理内容从原来的四个层面拓展到六大层面。

近年来,国内的软件工程学者也越来越关注项目风险管理研究问题。在 2001 年 5 月,中国优选法统筹法与经济数学研究会项目管理研究委员会正式提出了中国的项目管理知识体系文件《中国项目管理知识体系》(C-PMBOK),以项目生存周期为主线,以模块化的形式来描述项目管理所涉及的主要工作及其知识领域。其中对项目风险管理规

范进行了详细描述，该知识体系是项目管理规范化运作的理论基础和技术指南。

1.2.2 IT 项目全生命周期

由于 IT 项目具有技术含量高、项目周期长、牵涉部门多、项目不确定性大等特点，因此将 IT 项目分划为几个阶段，有助于我们对项目中风险的进行管理。但由于 IT 项目种类有很多，不同行业的项目生命周期阶段划分也不完全相同，而且如果从广义和狭义两个方面来定义 IT 项目全生命周期也有很大的差异，因此本文按项目管理共性对 IT 项目全生命周期进行阶段划分。

IT 项目的全生命周期(total life cycle of IT project , TLCITP) 是指从 IT 项目启动到项目收尾的整个过程，可分为前半生命周期和后半生命周期。前半生命周期主要工作是做计划，称作 IT 项目可行性阶段，包括 IT 项目概念阶段、需求分析阶段、方案设计等阶段。后半生命周期主要是项目实施工作，称作 IT 项目获取阶段，包括项目设计开发、项目实施、维护、收尾等阶段。一个 IT 项目在开始下一个阶段前，必须确保成功完成本阶段的工作。这种 IT 项目全生命周期的方法可以更好地对项目风险进行控制^[7]。

而 IT 项目全生命周期风险管理则是利用系统工程的理论方法对整个 IT 项目全生命周期中的风险进行识别、分析、评价、规划、控制、跟踪等持续改进的管理过程。文中提出的 IT 项目全生命周期的基本框架如图 1-1 所示。

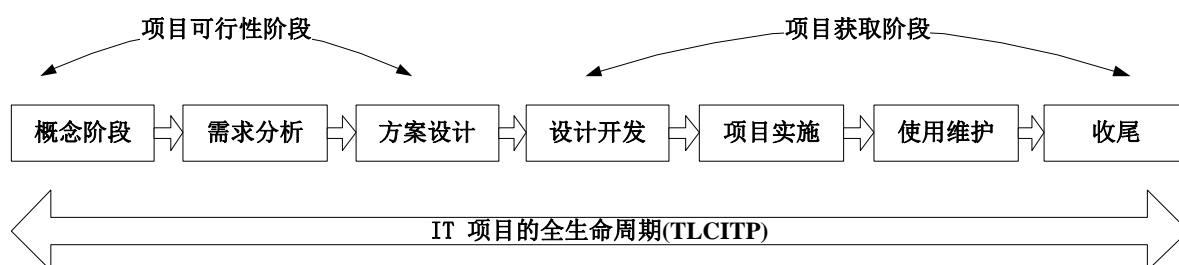


图 1-1 项目全生命周期基本框架

（资料来源：王寓辰，张金隆，卢新元，陈艳．全生命周期下 IT 项目风险识别研究．管理学报，2005 年第 9 期）

1.2.3 全面风险管理体系

全面风险管理体系是公司在风险管理活动中建立并维护的必要系统，包括指导公司整体风险管理活动的风险管理策略、执行风险管理功能的风险管理的组织职能体系、为保证风险管理顺利执行的内部控制系统、用于提高风险信息收集、分析、传递的效率和效果的风险管理信息系统以及风险理财措施五个组成部分。从而为实现风险管理的总体

目标提供合理保证的过程和方法。

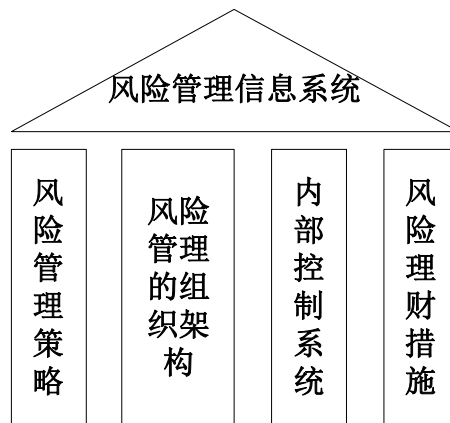


图 1-2 全面风险管理体系

（资料来源：本研究整理）

全面风险管理体系需要对企业各种风险进行统一、集中的识别、排序和控制，需要建立科学的全面风险管理流程，保证企业全面风险管理工作的有序性和有效性。是公司开展风险管理活动的基础，而这一体系的初始搭建也需要通过执行全面风险管理程序获得。

（1）风险管理战略

风险管理战略是根据公司整体经营战略制定的全面风险管理的战略，是指导公司风险管理活动的方针和行动纲领，是针对公司面临的主要风险设计的整套处理方案。清晰的风险管理战略是促使全面风险管理体系有效运行的关键。

风险管理战略包括公司的风险偏好和风险承受度、风险度量模型、全面风险管理的指导方针、全面风险管理的资源配置和风险文化等几个组成部分。

（2）风险管理的组织架构

风险管理的组织架构是风险管理的具体实施者，是全面风险管理体系的核心。通过合理的组织结构设计和职能安排，可以为有效项目风险管理提供基础。风险管理组织架构决定了公司监控、评估和规避风险的能力，它的目标是保证与公司的风险管理战略顺利实施。

风险管理组织体系主要包括公司法人治理机构，风险管理部门、内部审计部门、持续控制部门、其他有关职能部门及其职责，各相关业务单元的领导组织机构及其职责。

（3）内部控制系统

风险管理内部控制系统作为全面风险管理体系的其中一部分，通过完善公司的内部

控制环境，为公司提供纪律和架构，塑造公司文化，影响员工的控制意识，形成人岗匹配、授权有度、运行有序、监控到位的环境。规范公司管理行为，明确管理职责，控制公司各项经营活动过程中可能出现的风险，确保公司整体目标的最终实现。

内部控制活动贯穿于整个公司内所有级别和职能部门，包括批准、授权、查证、核对、经营业绩评价、资产保全措施和职责分工等一系列活动，具体体现为公司的业务和管理流程。实施有效的控制活动，以风险防范和控制为出发点，结合风险评估结果，按照手工控制与自动控制、预防性控制与发现性控制相结合的原则，综合运用各类控制措施，可以将风险评估过程中识别出的风险控制在可承受范围之内，保证企业战略目标、经营目标、报告目标以及合规目标的实现。

内部控制体系是风险管理的关键，是风险管理实际操作的核心，内控体现的完整性、准确性和有效性直接决定了具体风险管理的效果。通过内部控制达到有序和有效率的经营、可信赖的财务报告和符合法律的公司法规这三个目标，另外，全面风险管理还期望达到与公司整体战略目标相结合的风险最优化以及保护公司不致因灾害性事故遭受重大损失这两个目标。但是，内控目标的局限在于与公司的战略目标联系不紧密，主要将着眼点放在风险防范上。

（4）风险管理信息系统

风险管理信息系统是管理信息系统中必不可少的系统，管理人员由此认识并处理现实的或者潜在的风险，以抵御风险所产生的不利效应，降低风险成本。

风险管理信息系统能够进行各种风险的统计和定性分析、定量分析；能够实时报告风险矩阵、重大风险和重要业务流程的监控状态；能够对超过风险预警上限的重大风险进行信息报警；能够满足风险管理内部信息报告制度和公司对外信息披露管理制度的要求。

风险管理信息系统实现在各业务部门、单位之间信息集成与共享，既能满足单个项目业务风险管理的要求，也能满足企业整体和跨职能部门、业务单位的项目群风险管理的要求^[10]。

风险管理信息系统是实施全面风险管理不可缺少的信息系统，是各个子系统的信息集成，是公司高效率风险管理的必要工具。风险管理信息系统为量化风险提供历史数据参考，并且根据项目开展过程中具体的风险事件进行定量分析。

（5）风险理财措施

风险理财措施是指企业运用金融手段来管理、转移风险的整套措施政策和方法。风险理财的方式包括风险准备金和购买保险。随着金融市场的发展和风险防范意识的不断提高,风险理财手段也在不断增加,包括各种金融衍生品等,为风险的转移、分担、应对、补偿提供了工具。

另外,可以关注在现有管理条件下如何选用风险理财的方式,以及如何管理使用各种风险理财手段本身的风险。另外,要关注风险理财方面的人才储备,为实现公司的持续风险管理奠定基础。

1.2.4 经典风险管理理论

软件项目风险是指在软件项目过程中遇到的成本和进度风险,并且可能对项目质量产生影响。风险管理是项目管理的重要内容之一。在进行软件项目风险管理时,首先要识别风险,评估风险出现的概率及产生的影响,然后规划风险应对措施,不断跟踪风险的应对效果和对项目的影响。软件项目风险会干扰项目计划,影响项目实施,如果项目风险变成现实,需要增加项目资源,甚至导致系统不能上线。

IT 软件项目风险管理在国外开展的比较早。一方面,在基于过程研究风险管理方面的模型,比较有名的是 Boehm 提出的 Boehm 模型。美国在卡内基·梅隆大学设立的软件工程研究所 (Software Engineering Institute: SEI) 提出的连续风险管理 (Continuous Risk Management: CRM), Microsoft 公司提出的微软解决框架 (Microsoft Solutions Framework: MSF) 等。

1. Boehm 体系

1989 年 Boehm 提出软件风险管理体系后,又于 1991 年详细描述了他的思想体系。Boehm 定义风险的公式

$$RE=P(UO)*L(UO)$$

其中 RE 表示风险或者风险所造成的影响;

P(UO)表示令人不满意的结果所发生的概率;

L(UO)表示糟糕的结果会产生的破坏性的程度;

在风险管理步骤上,Boehm 基本沿袭了传统的项目风险管理理论,指出风险管理由风险评估和风险控制两大部分组成,风险评估又可分为识别 (identification)、分析 (analysis)、设置优先级 (setting the steps of priority) 3 个子步骤,风险控制则包括制定管理计划 (making management plans)、解决 (solving) 和监督风险 (monitoring risks) 3

步。

Boehm 思想的核心是 10 大风险因素列表，其中包括人员短缺、不合理的进度安排和预算、不断的需求变更等。针对每个风险因素，都给出了一系列的风险管理策略。在实际操作时，以 10 大风险列表为依据，总结当前项目具体的风险因素，评估后进行计划和实施，在下次定期召开的会议上再对这 10 大风险因素的解决情况进行总结，产生新的 10 大风险因素表，依此类推。

10 大风险列表的思想可以将管理层的注意力有效地集中在高风险、高权重、严重影响项目成功的关键因素上，而不需要考虑众多的低优先级的细节问题。而且，这个列表是通过对美国几个大型航空或国防系统软件项目的深入调查，编辑整理而成的，因此有一定的普遍性和实际性。但是它只是基于对风险因素集合的归纳，尚未有文章论述其具体的理论基础、原始数据及其归纳方法。另外，Boehm 也没有清晰明确地说明风险管理模型到底要捕获哪些软件风险的特殊方面，因为列举的风险因素会随着多个风险管理方法而变动，同时也互相影响。这就意味着风险列表需要改进和扩充，管理步骤也需要优化。

2. SEI 体系

SEI (Software Engineering Institution) 是世界上著名的在改善软件工程管理实践有突出表现的组织，其对风险管理投入了大量的研究。SEI 提出了持续风险管理模型 CRM (Continuous Risk Management)。1999 年前后分别以技术报告和手册等形式公布了基于分类的风险辨识(TBQ)、连续风险管理(CRM)、软件风险评估(SRE)、软件采购风险管理成熟度模型(RM 2CMM)和团队风险管理(TRM)。整体思想是想以 TRW 为框架和以 TBQ 等为基本手段，依托 SRE 过程及贯彻 CRM 思想，配合软件能力成熟度模型(SW 2CMM)和软件采购成熟度模型(SA 2CMM)，从而完成软件的风险管理。^[50]

SEI 的风险管理原则是：不断评估可能引起不良后果的风险；决定最迫切需要处理的风险；实施控制风险的策略；评估并确保风险策略实施的有效性。其中，CRM 模型要求在项目生命周期的所有阶段都关注风险识别和管理，它将风险管理划分为 5 个步骤：风险识别 (Identification)、分析 (Analysis)、计划 (Planning)、跟踪 (Tracking)、控制 (Control) 的活动闭合环，风险识别主要依靠问卷完成，涵盖了大概 200 个问题，涉及 13 个主要领域。风险分析主要是分析每个风险在项目过程中发生概率和后果严重性，总结出最严重的十大风险问题。风险计划是规划项目风险的应对方案：风险管理步骤、风

险负责人和职责、管理行为和结束的时间，还要确定风险处理的优先级，项目风险整体管理计划。风险跟踪是跟踪风险应对的效果并汇报十大风险问题当前的状态，其目的是收集准确的、及时的风险数据，并及时报告给项目管理层。风险控制是发现风险后根据风险管理计划进行及时有效的风险决策，分析进行风险跟踪后给出的风险状态信息，确定需要采取什么样的风险管理行为，并给出行动方案。

SEI 和 Boehm 的模型都以风险管理的过程作为主体，研究每个步骤所需的参考信息及其操作。而 Aalborg 大学提出的思路则是以 Leavitt 模型为基础，着重从引起软件开发风险的不同原因出发探讨风险管理。

3. SEIRM(Software Engineering Risk Model)模型

SEIRM 从技术和商业两个角度对软件风险管理进行剖析，考虑的问题涉及开销、进度、技术、性能等。同时还提供了一些数据、指标和模型来估计和预测风险，由于这些数据来源于大量的实践经验，因此具有很强的说服力。

该模型的主要目的是识别、分析、交流和规避技术风险。技术风险包括：潜在的设计、代码、实现、验证和维护的问题；二义性，技术不确定性，过时的技术和主要的边缘技术。采用分类的方法和基于分类的问卷来识别开发中的商业风险，商业风险包括：市场风险，产品风险，管理风险和预算风险。

优点：提供的有关风险管理的数据来源于大量的实践经验，证实了以前实践中的经验对以后软件开发项目所起的重要作用，具有重要的指导意义和实施开发的依据。

缺点：风险管理经验的获取需要一定的时间积累，对于新公司或开发不规范的公司来说，没有经验数据的积累减小了其适用范围。^[49]

4. MSF 风险管理过程

MSF 风险管理原则主张前瞻性的风险管理、持续的风险评估以及项目生命周期的决策集成。风险被持续地进行评估、监控和积极地应对，直到风险消除或是转化为积极风险为止。MSF 风险管理定义了项目团队管理现有的风险，计划和执行风险管理策略以及为企业获取知识过程中的六个逻辑阶段。这六个阶段分别是：识别，分析和分级，计划和调度，跟踪和报告，控制和学习。

优点：基于前人的项目风险管理经验，吸取经验教训，减少现阶段风险的发生概率，有力的证明了前人的项目经验对今后的风险管理有重要指导意义。

缺点：团队合作和沟通是现在项目管理当中非常重要的组成部分，项目的成功与否

和项目干系人之间是否进行有效的沟通非常重要，尤其是在当今的软件项目管理中更是如此，而在该模型中没有很清楚的表达出来。^[49]

以上 4 套体系总体都是偏重解决开发活动内部的技术风险，其风险控制手段也往往着眼于降低风险发生的可能性，对如何规避风险后果措施不多。

1.3 研究内容与方法

1、研究内容

随着金融业的迅猛发展，业务变的日益复杂，IT 业务系统功能越来越多，系统逐渐庞大复杂。在面向金融公司 IT 项目风险管理研究相对缺乏的情况下，将全生命周期风险管理理论应用于金融公司的 IT 项目运作之中，也就是本文所要阐述的内容。全生命周期风险管理，就是对项目从其需求分析、可行性分析、开发实施到项目收尾的全过程进行宏观统筹的风险管理。

本文以全面风险管理理论、生命周期理论作为理论基础，结合 F 公司 IT 项目风险管理的实践案例，提出了 F 公司软件项目全生命周期风险管理模型，并进行了详细阐述。应用解释结构模型分析 F 公司在软件项目过程中所存在的各种风险因素之间的关系以及风险产生的根源。并且对 F 公司的软件项目关键风险及规避关键风险的实施方法进行了深入探讨和分析。

2、研究方法

本文从大量前人研究实践中概括提炼，并借鉴国内外经验，主要采用的研究方法有以下几种，主要特点是将理论与实践结合并进行集成创新。

(1) 理论与文献研究。本文研究的重要方法是查阅文献和理论研究。在全文研究过程中，查阅了国内外有关风险管理、项目生命周期管理、战略管理、项目管理等领域的有关文献，从而得以站在前人的研究基础上来思考问题。本文的研究综述、结构体系和风险管理模型的形成是文献研究与理论研究方法的直接成果体现。

(2) 定性与定量研究方法的结合使用。定性研究与定量研究的主要区别在于认识问题的途径和方法手段的不同。定性研究发展趋势，主要大量采用管理学、叙事研究等研究方法，其主要表现方式大都为案例、访谈纪要等；定量研究主要采取数据分析、建模分析等，其主要表现方式大都为图表。在风险分析中使用了 ISM 解释结构模型进行定量分析。

(3) 案例研究。理论必须与实践相结合，才能使论题更具有实际意义。本文在理

论论述中，引用了案例来对相关问题进行说明。例如，以 F 公司软件项目为例对风险识别分析等问题进行了案例分析。

另外，在本文中还运用了类比、对比、归纳、演绎等多种方法，并且也适当融合了相关学科各自的工具和手段来对论题进行系统分析。

1.4 论文结构和创新点

1、论文框架

本文围绕 F 公司的软件项目风险管理问题展开，首先提出了面向 F 公司的项目风险管理模型。这个模型是从现有的研究资料和金融行业软件项目的特点总结归纳而来，得到风险管理理论和生命周期理论的支持。然后结合 F 公司的软件项目风险管理案例，对项目涉及的各种风险及相互关系进行分析，并提出有针对性的实施建议。本文最后针对上述分析得出的若干关键风险进行了详细的描述和深入的剖析，并提出了具体的规避措施。这将使得本文的研究成果，面向 F 公司的项目风险管理模型从理论基础，到实际应用等一系列的问题得到贯通，寻找出一条为 F 公司解决项目风险管理问题的解决方案。研究框架如图所示：

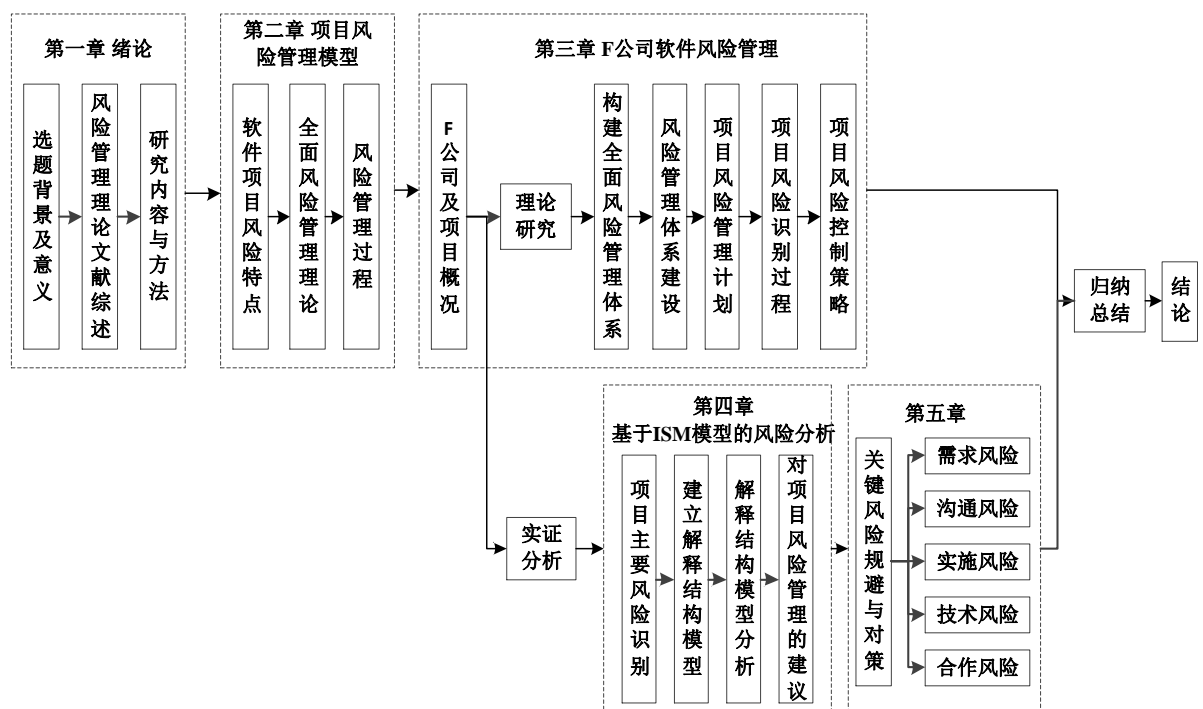


图 1-3 研究框架

（资料来源：本研究整理）

第一部分，绪论，介绍论文的研究背景、意义，以及研究内容与方法等。

第二部分，结合金融行业软件项目的特点，论述全生命周期项目风险管理模型，并对项目风险管理的具体实施进行详细的分析。

第三部分，以 F 公司软件项目为例，应用理论结合实际的方法，提出了面向 F 公司的全生命周期风险管理模型。介绍 F 公司软件项目风险管理的制度建设，风险管理计划制定，风险识别和风险控制策略。

第四部分，应用 ISM 模型对项目中的主要风险因素进行了具体的分析，并提出了实施建议。

第五部分，通过上一部分的分析得出影响项目的若干关键风险，在该部分进行了进一步的分析和描述，并提出了具体的规避措施。。

这五部分内容相互支持，让本文的研究成果从理论到实际再到成功应用，探索出解决中小金融机构 IT 软件项目过程中需要面对的风险管理问题。

2、本文创新点：

本文的创新之处有三点：

(1) 在 F 公司 IT 项目风险管理案例分析的基础上，引入全生命周期和持续风险管理，提出了面向中小金融机构的 IT 项目风险管理模型。将风险管理过程由分块管理变成整理风险管理，项目过程中对风险管理进行持续控制并及时更新风险管理计划，由被动变为主动。

(2) 使用 ISM 解释结构模型分析 F 公司项目风险之间的层级关系，分析得出 F 公司软件项目的风险解释结构，总结出最需要关注的根源风险和直接风险。并针对性地提出了风险管理建议。

(3) 针对 F 公司软件项目实施过程中，存在许多风险问题，本文分析了几个关键风险，对风险产生的原因进行了分析，并且对如何避免这些风险提出了具体的规避措施。

本文的研究分析对中小金融公司 IT 部更好地管理软件项目风险具有借鉴意义。

第二章 项目风险管理模型

通过分析金融公司项目风险的特点，应用理论结合实际的方法，提出了针对 IT 项目的全生命周期风险管理模型，并对软件项目风险管理过程进行详细论述。

2.1 软件项目风险特点

中小金融公司作为非银行业金融机构，业务开展高度依赖 IT 系统，软件项目出现风险后，将导致系统不能按时上线，可能导致业务不能正常开展，容易产生金融业务风险，给客户不良的影响，因此软件项目风险管理显的尤其重要。此外，金融行业公司要受到人民银行和银监会的监管，业务操作风险和信息系统安全都要符合相关规定，特别是在近今年金融市场火爆的情况下，各种业务开展非常普遍，系统稳定和信息安全是确保业务顺利开展的首要条件。软件项目的开发实施过程中，要特别关注项目风险管理，风险控制，同时信息安全和操作风险要符合相关的监管要求。

随着 IT 项目规模越来越大，项目复杂度和管理难度随之不断提高，项目团队能否有效解决项目执行过程中出现的各种问题已成为影响项目效果的关键。项目通常在需求、开发、使用、维护等各个阶段都存在大量的不确定性因素，从而在整个生命周期中都时时刻刻伴随着风险。项目中的风险主要具有以下几个特点：

（1）随着不断发展的业务，引起需求不断放大变更，企业面的环境变化，都导致了项目的不确定性。由于金融公司软件项目涉及到的单位和部门相对比较多，项目开展环境比较复杂，个性化的业务创新程度比较大，并且随市场迅速变化，往往可能在一个项目周期内出现很多需求变更，增加了项目的不确定性，添加了项目管理不确定性风险。

（2）金融企业中 IT 系统是业务发展的核心平台，项目成果需要尽快投入适用，满足客户需求，提供各种金融服务。个性化的软件项目往往有一定的时间约束，以较短的时间产生优质高效的系统，这对项目的进度控制提出了较高的要求。

（3）金融软件项目多与现有业务系统密切相关，新增的软件项目与现有业务系统之间普遍存在数据交互。因此在系统需求分析，软件设计，开发，测试过程中需要细致全面，着重关注项目相关性。项目实施过程中风险管理格外重要，既要确保项目自身的质量，还要确保企业正常提供服务，要防止对相关的业务系统产生影响。

(4) 金融公司在软件项目实施过程中, 信息安全需要符合审计要求, 系统的操作风险要满足监管部门(银监会)的监管要求。如: 在系统建设过程中开发部门, 业务部门不能承担项目的运维工作, 系统维护要交给独立的运维部门进行维护。项目中需求分析, 代码开发和上线实施等各个阶段的文档都需要存档备查, 外包公司需达到监管部门要求的资质。

(5) 公司高管对 IT 项目管理的重视度不够, 公司高级管理层的决策更多地关注金融产品, 新业务的开发, 而 IT 运营方面除非出现了重大的问题, 否则高级管理层很少触及。因此, 对高级管理层而言, IT 运营风险相对于其他风险来说要疏远的多。

(6) 在项目全生命周期内, 项目风险具有客观性和普遍性的特征, 也就是说在有限的空间和时间内, 项目管理人员可以对项目风险进行控制, 但是不能完全消除所有风险。

(7) 在整个项目运作过程中由外部环境因素和人为控制的原因, 风险在质和量上都会发生变化, 同时项目的不同阶段都可能出现新的风险。

(8) 虽然项目开展过程中, 个别风险事件的发生带有偶然性, 但我们对大量风险事件的统计分析后, 发现风险却呈现明显的规律, 所以可以在项目过程中借助概率统计方法或者其它风险分析方法来分析并控制风险。

2.2 全面风险管理理论

所谓全面风险管理, 是指围绕公司经营目标, 在公司的各个管理过程中执行风险管理的基本流程, 为主体的目标实现提供合理保证, 是渗透到企业的各种活动的持续或者反复的相互影响的过程。主要是培育良好的风险管理文化, 建立全面风险管理体系, 包括风险管理环境、风险目标设定、风险因素识别、风险应对和控制活动、信息与沟通、风险监控等, 从而为实现风险管理的目标提供全面保证的过程和方法。全面风险管理不是一个严格的顺次过程, 一个构成要素并不是仅仅影响接下来的哪个构成要素, 它是一个多方向的, 反复的过程, 在这个过程中几乎每一个构成要素都能够影响其他构成要素。

全面风险管理需要对各种风险进行统一、集中的识别、分析和控制, 建立科学的全面风险管理流程, 保证全面风险管理工作的有序性和有效性。全生命周期风险的管理是建立在当前项目风险管理的各种理论、方法的基础上, 其中包括一些定性和定量的方法、动态系统的方法等。

2.2.1 项目全面风险管理

软件项目全面风险管理是由若干风险管理要素组成的一个有机整体，这个体系可以将风险收益，风险偏好和风险策略紧密结合起来，增强风险的应对能力，尽量减少风险造成的损失；准确判断和管理叠加风险，提高对各种风险的整体反应能力；最终能根据风险带来的影响科学地分配项目资源，控制项目风险，确保 IT 项目顺利开展。可以从以下几个方面理解 IT 项目全面风险管理：

(1) IT 项目全面风险管理是一个持久过程。通过在企业项目管理的各个过程中执行风险管理的基本流程，培育良好的风险管理文化，建立健全全面风险管理体系，包括风险管理环境、风险目标设定、风险因素识别、风险应对和控制活动、信息与沟通、风险监控等，从而为实现风险管理的总体目标提供合理保证的过程和方法。^[10]

(2) IT 项目全面风险管理需要依靠全体员工。不仅需要建立大量的风险管理制度政策，而且需要 IT 项目的经理、各级管理人员积极参与，参与的人员会形成了风险管理文化、风险偏好、风险管理目标和政策，风险管理活动也必须依靠全体员工才能顺利开展，重视全员风险管理对项目管理非常重要。^[10]

(3) IT 项目全面风险管理覆盖了 IT 项目各环节的所有风险。其中包括进度风险、技术风险、沟通风险、合作风险等等。全面风险管理就是要对这些影响 IT 项目目标的风险进行系统识别，评估，分析，报告和处置，它需要考虑 IT 项目所有环节的行为，从战略规划和资源分配，到各单元模块管理，风险都需要得到有效控制。^[10]

2.2.2 项目全生命周期风险管理

在项目全生命周期管理中概念阶段，项目的相关利益体、项目范围控制、技术水平不清晰以及资金情况把握不准是项目风险存在的主要因素；进入项目规划阶段，随着项目规划的制定、项目资源的分配、项目成本预算和进度安排，项目决策风险逐渐减弱，项目进度安排、管理风险逐渐突显；实施阶段大部分问题都会表现出来，主要包括挣值分析进度与成本的偏差评估、项目计划的更改、资源配置修改、项目范围的变更等风险；到了收尾阶段，项目预期成果和目标如果没有满足利益主体的要求，仍存在一定的风险。

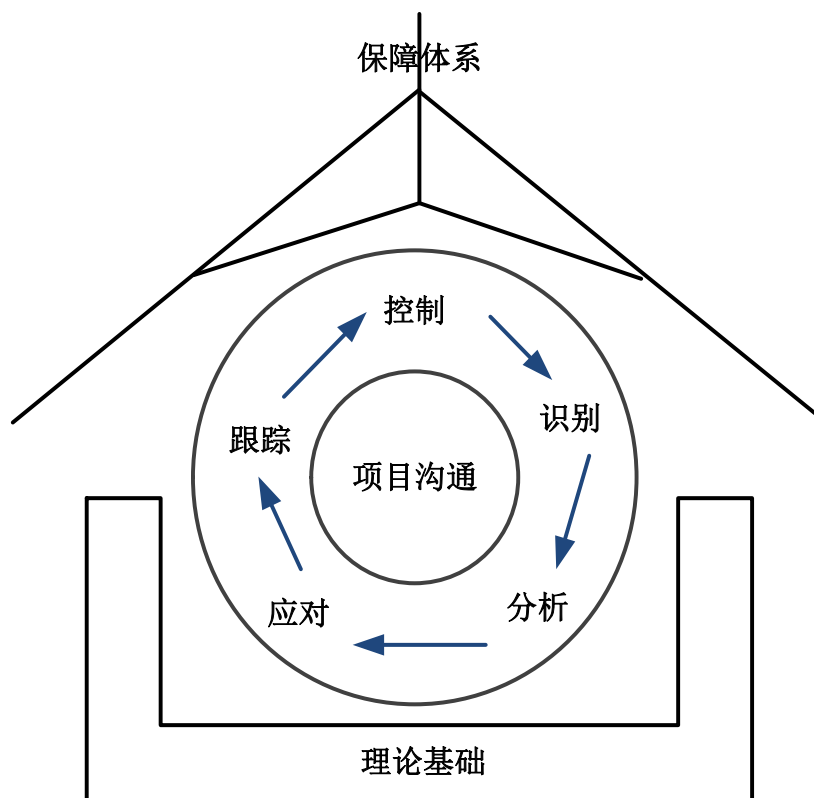


图 2-1 全生命周期风险管理体系框架

（资料来源：方德英，李敏强．IT 项目风险管理理论体系构建．合肥工业大学学报(自然科学版)，2003 年第 8 期）

全生命周期风险管理的最重要的特征就是持续的风险管理，是风险全生命周期管理的核心，在对风险系统认识的不断深入的基础上，借助于理论方法、团队的组织管理以及信息技术来完成从识别、分析、应对、跟踪及控制的反复循环的动态过程。图 2-1 是持续风险管理的过程示意图。可以看出，持续的风险管理是项目全生命周期中不断重复的过程，图中的箭头标识了信息的逻辑流，而沟通是信息流的核心和手段，其具体活动如下^[6]：

（1）风险识别(Identify)，要了解项目面临的风险有哪些，他们各自的风险因素是什么，如果发生会有什么后果，其中会导致风险事故的原因有哪些等内容。可以借助概率风险评价(PRA) 方法以及事件和故障树(FTA)等技术。

（2）风险分析(Analyze)，重点对项目的单个风险因子进行估计或量化，对项目所有不确定性和风险要素全面系统地分析风险事件发生的类别、概率和对项目的影响程度。

（3）风险应对(Responses)，通过项目风险识别和分析后，使用特定的方法和技术处理已知的风险，识别谁应该对风险负责，并对因降低风险产生的成本以及进度方面的

影响做出评估。

(4) 风险跟踪(Track), 主要包括监视已经识别风险和可能突发风险的状态, 对风险的进展状况进行记录和跟踪, 便于及时发现和解决突发问题。记录的内容主要包括, 风险识别人员、风险的影响范围、发展情况、是否采取规避措施、风险负责人员等。

(5) 风险控制(Control), 系统化的风险追踪过程, 也是运用已经建立的标准体系评估风险应对效果的过程。通过采取一定措施和方法, 降低风险事故发生的概率, 减小风险事故对项目的影响。

(6) 风险沟通(Communicate), 项目成员通过正式或非正式的沟通渠道来了解项目有关重要风险的状态、项目活动以及将要出现的风险的信息。

每个风险因素一般都需要按顺序经过这些活动, 对不同的风险因素开展的不同活动可以是并发的或者交替的。风险管理活动在整个项目生命周期内呈现连续性、并行性、迭代性。处于风险管理体系框架上方的风险保障体系需要依托于企业管理组织结构和项目管理体系, 至少需要组织保障和制度保障, 从行政制度、技术方法和知识上确保风险管理体系的完整性。

2.3 风险管理过程

在软件项目风险管理体系中, 项目风险管理主要包括五个过程(识别、分析、规划、跟踪、控制)。金融公司都会设立独立的项目管理部门(PMO), 对软件项目进行统一项目管理, 风险管理和项目控制, 并由项目管理部门的人员担任整个软件项目的项目经理。

作为金融行业公司, 对软件项目的最终实施、维护的流程非常重视, 在软件项目实施过程中由独立的运维部门(OP)来完成此项工作。金融软件项目相关性强, 运维部门在项目实施过程中, 会通过持续控制部门对项目实施过程进行风险识别和分析, 并由项目经理负责制订实施方案, 在交由专家组进行审核, 评估, 并按照金融业风险管理的要求完善方案细节。然后在此基础上对实施方案进行实施测试, 进一步验证方案的可行性, 可操作性, 并制定相应的应急方案, 回退方案进行风险控制。在测试成功后, 才能进行实施上线, 上线后通过监控, 运维分析, 系统满足银行业安全监管要求后, 将进一步安排后续系统推广, 系统维护工作。

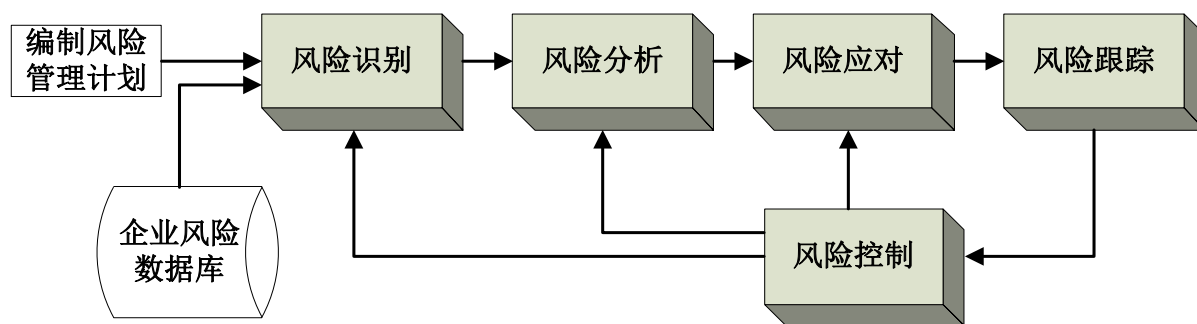


图 2-2 全生命周期项目风险管理过程

（资料来源：本研究整理）

2.3.1 编制风险管理计划

风险管理计划是一份针对项目全生命周期内的风险管理程序的计划文档，包括实施项目风险管理的目标、策略和方法。该计划描述了风险识别、分析、评估及控制过程的所有方面的内容。

风险管理计划是确定如何实施项目风险管理活动的过程，对项目有价值的风险管理的实施方法。可以确保风险管理的程度、类型和可见度与项目对组织的重要性相匹配。规划风险管理的重要性还在于为风险管理活动提供充足的资源和时间，并为评估风险奠定一个共同认可的基础。

风险管理计划概况了一个特定项目将如何进行风险管理。像其他专门的知识领域计划一样，风险管理计划也是项目管理计划的一个子集。风险管理计划活动与项目计划和进度活动相互联系的，因为风险存在于项目开始到项目完成的所有阶段，在项目过程中应该分派和指定专门资源来积极管理风险。

2.3.2 风险识别

风险识别是采用系统化的方法，使用多种技术识别项目中潜在的威胁和风险，为项目管理团队创建一个潜在的风险列表，该列表需要覆盖项目的所有领域，并通过提供足够信息进行风险分析。便于制定规避风险和降低风险的计划和策略。风险只有被识别并准确地表述出来，项目管理团队才能决定采用风险分析的方法，进而进一步对风险进行分析和计划并进行风险控制。风险识别是一项反复的过程，应该在 IT 项目的生命周期自始至终定期进行。风险识别包括识别风险的来源、分析风险产生的原因、描述风险的特征和确定风险的影响范围。风险的识别具体分为三步：收集资料、评估项目面临的风险形势、根据各种项目状态将潜在的风险识别出来^[20]。

(1) 风险识别过程定义

风险识别过程是弄清哪些潜在事件会对项目有害或者有益的过程。风险识别过程可以看作是一个系统，风险的来源分为项目内部和项目外部。项目经理只负责管理项目内部风险，如某个项目团队成员没有经过充分的培训，或者某个技术的应用出现了困难，那么项目的目标，也就是范围、进度和预算都会受到影响，会阻碍项目目标的实现。

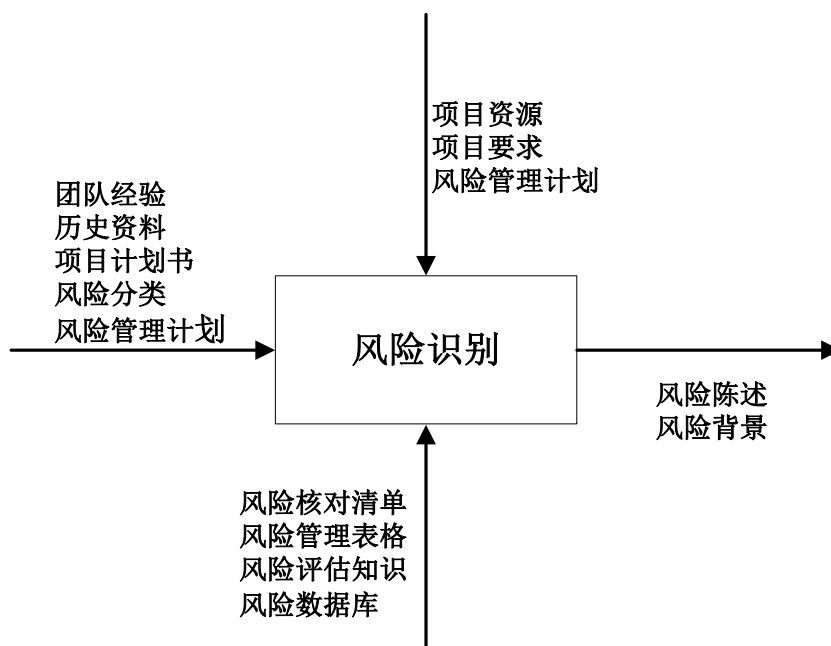


图 2-3 风险识别过程定义

(资料来源：本研究整理)

风险识别依据：包括项目章程，风险管理计划，项目产品说明书，项目所有计划编制输出(比如，WBS，资源计划，采购计划，费用计划，进度计划等)，项目约束条件和假定，历史资料，风险数据库信息。

风险识别过程：确定目标划，明确最终的参与者，收集资料，估计项目风险形势，根据直接或者间接的症状将潜在的项目风险识别出来，运用检查表，流程图，头脑风暴法，情景分析法，德尔非法、SWOT 分析法、历史风险核对表等。但这些都是非结构化的，均有主观性。也需要结合结构化的方法，比如对任务的分解，对 WBS 中的每个分解任务进行风险识别，或者对项目中不同领域中可能存在的风险进行识别。

风险识别成果：

- 1) 已识别的项目风险：已识别的项目风险是项目风险评估的最重要结果，它通过定性的项目风险清单来表示，该清单对项目风险的描述应该尽量简单，容易理

解。

- 2) 潜在的项目风险：潜在的项目风险是指没有迹象表明会发生的风险，但是人们可以主观判断预见的风险，如重要技术专家的流失。当然，潜在的项目风险可能会发展成为项目的真正风险，因此要给予足够的重视。项目管理者应该根据风险来源进行适当的分类，并以表格或文字进行清楚的描述，编制出潜在的项目风险清单，为风险管理的后续过程打好基础。
- 3) 对项目管理其他方面的改进：在项目风险识别的过程中，可能会发现项目管理其他方面存在一些问题，借此机会可以进行修改和完善。

(2) 风险识别活动

风险识别过程是寻找风险、描述风险和确认风险的活动过程。项目风险识别过程一般可以分为以下四个步骤。

1) 确定目标

项目风险识别的目标就是要识别可能发生的消极事故，这个目标非常明确。但是每个项目的性质有差异，项目合同类型也不同，那么项目风险管理的目标也不相同。应该根据项目管理计划，项目干系人，项目发起人和外包公司一起确定本项目的风险管理目标和范围。

2) 明确风险识别干系人

根据项目风险管理的目标和范围，确定参与项目风险识别的干系人。项目风险识别需要项目干系人一起参与，项目管理人员不仅需要掌握项目的进度信息，还要了解项目干系人的背景资料，明确主要干系人。这些干系人应具有业务及技术方面的两方面的技能，干系人需要了解项目的目标及面临的风险，应具备沟通技巧和团队合作精神，乐于分享信息，这对项目风险识别是非常重要的。

3) 收集资料

项目风险识别需要收集的资料有以下几种。

项目产品说明书：项目具有不确定性，但是项目开展中遇到什么样的风险与项目目标有一定的关系。

事业环境和组织过程资产：可从查阅项目相关的管理计划或者风险管理数据库得到。

与本项目类似的案例：借鉴以前类似项目的经验和教训是识别项目风险的重要手段。

采访项目参与者：访谈以前参与类似项目的项目人员，收集项目风险相关的资料。

4) 估计项目风险形势

通过项目风险形式估计，判断和确定项目风险目标是否正确，是否具有现实性和可测性。根据项目成本和进度分析实现项目目标有多大的不确定性，理清项目开展有多少可用资源。

2.3.3 风险分析

对项目风险进行定性和定量评价，并依据风险对项目目标的影响程度进行风险分级排序的过程。通过系统分析和综合分析项目风险的各种因素，综合评估项目风险的影响范围。通过建立系统的项目风险评价体系，系统分析风险对项目范围的影响，^[4]并估算出各种风险发生的概率以及由此可能导致的损失大小，进一步确定项目的关键风险，挖掘影响项目风险的根本原因，为风险应对提供依据，以保障项目的顺利进行。

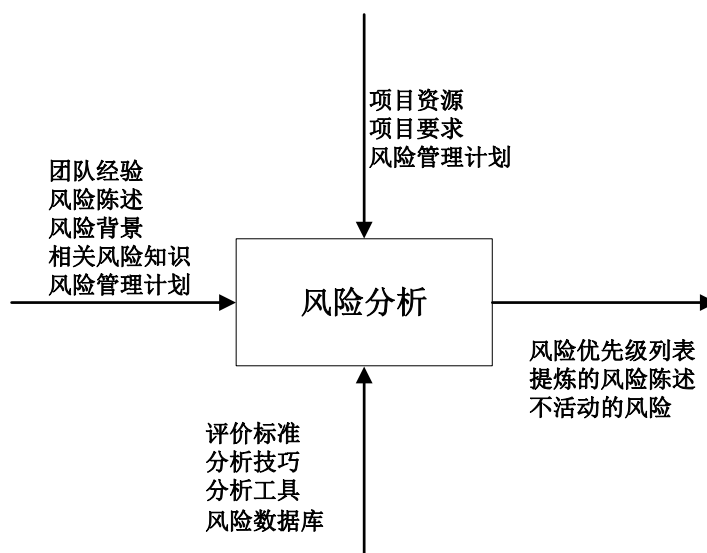


图 2-4 风险分析过程

（资料来源：本研究整理）

风险分析分为定性风险分析和定量风险分析。定性风险分析是一种对风险和条件进行定性分析，并按影响大小排列它们对项目目标的影响顺序的分析方法。定量风险分析是对通过定性风险分析排出优先顺序的风险进行量化分析。定量风险分析一般应当在确定风险应对计划时再次进行，以确定项目总风险是否已经减少到满意。重复进行定量风险分析反映出来的趋势可以指出需要增加还是减少风险管理措施，它是风险应对计划的一项依据，并作为风险监测和控制的组成部分。

通过 ISM 模型对软件项目的风险进行结构性定量分析，我们能清楚的分析出软件项

目过程中的风险间的因果关系。通过这样的因果关系的分析，我们才能清楚的找到在繁杂的风险因素中，什么因素才是重要风险的根源。

不同的风险发生后对项目造成的影响各不相同，主要有三个方面需要考虑。首先是风险的性质，即风险发生时可能产生的问题；其次是风险的范围，即风险的严重性及其总的分布；最后是风险时间，即何时能感受到风险及风险维持多长时间。据此确定项目的风险估计的概率，得到准确的风险估计。公司可以通过对风险量化、选择和排序，可以知道哪些风险是必须应对，哪些可以接受，哪些是可以忽略。公司在进行风险管理时候应该把主要精力集中在那些影响大、范围广、概率高以及可能发生的阶段性的风险上。

2.3.4 风险应对

风险规划是制定关于如何处理风险决策的过程。针对风险定性、定量分析的结果，来实施已经获得统一和资金支持的风险应对措施，以降低 IT 项目的风险的消极作用。在风险规划风险应对的过程中，需要根据风险的优先级来制定应对措施，并把风险应对所需要的资源和活动添加到项目的预算和项目管理计划中。

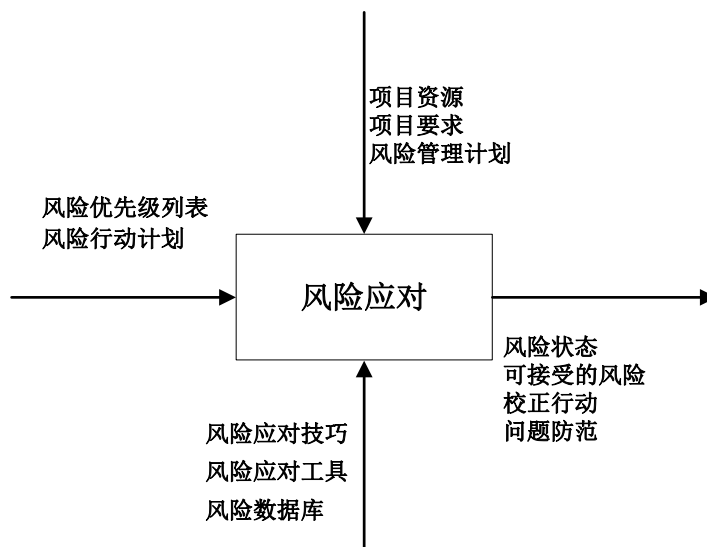


图 2-5 风险计划过程定义

（资料来源：本研究整理）

风险应对规划就是对已经识别的风险进行定性分析、定量分析和进行风险排序，制订相应的应对措施和整体策略。风险应对策略包括风险回避、转移、减轻、接受、开拓、分享、提高等。根据成本/收益原则以及风险分散原则采取最好风险解决方式。项目过程中有的风险可能会发生也可能不发生，有些风险可能一直都不会发生，有些风险也可能

被疏忽，以至风险后出现无法补救的情况都可能出现。因此，一般可以选择的风险应对有下面几种策略。

(1) 风险控制。软件项目中的风险控制是风险处理技术中最通行的一种，是对项目进展的状态进行连续跟踪和纠正的过程。它往往要采取审查、确定风险控制程度，确定最低可接受的风险及其他类似的管理措施。控制风险要制定一个有针对性的风险降低计划并跟踪其执行情况。项目风险管理人员想办法将负面风险事件的影响降到最低的可承受程度。尽早采取风险应对措施，可以降低风险发生的概率或风险对项目的影响。

(2) 风险承担。指项目风险保留在风险管理主体内部，通过使用内部控制措施等来减轻风险或者对这些的项目风险不采取任何措施。风险承担与其他风险对策的根本区别在于：不改变风险的客观属性，也就是不改变项目风险的发生概率，不改变项目风险潜在影响的严重性。企业需要准备风险基金以承担风险损失。风险承担既可以是有主动的，也可以是被动的。主动风险承担是风险管理者知道风险的存在，估计到该风险造成的损失程度，决定使用项目内部的资源来对损失实施弥补的措施。在有计划的风险承担中对风险损失的处理有许多种方法，比如会立即将其从现金流量中扣除，或者将损失分摊到较长的一段时间内，以减轻对单个财务年度的损失^[19]。被动承担则是指在识别和评估风险带来的影响失败的情况下，只有被迫承担风险带来的后果的处置方式。被动承担是风险管理者发现及时发现风险，一种被动的处理方式，往往会造成比较严重的后果，使项目遭受重大损失。

(3) 风险转移。软件项目可以选择用分摊风险的方法来降低风险。公司设法将某风险的结果和对风险应对的权利转移给第三方，如外包、购买保险等。其中外包就是把工作转让给别人，从而把有关的风险转移到别人身上。购买保险是由保险公司来承担风险的后果，在国内还鲜有其例，但这已经表现出一种趋势，也能够对双方能力进行约束。通过转移方式处置风险，软件外包企业面对的风险本身并没有减少，只是风险承担者发生了变化。

(4) 风险回避。风险回避是指当项目风险产生的概率很大，不利影响也很严重，在没有其他风险应对方法的时候，主动放弃项目或者改变项目目标，从而规避风险的一种策略。风险回避的优点有以下两个方面：第一、在风险产生之前，通过风险回避的方式在风险出现之前就将风险规避掉，大大降低了风险发生的概率。有

效避免了项目可能受到的影响；第二、节省了项目资金和人力成本，减少不必要的浪费，使得企业正面应对风险的成本降低。但风险回避有不足之处。风险回避可以分为积极的主动预防风险和消极的完全放弃两种。主动预防风险是指从风险源入手，将风险彻底消除。完全放弃是最彻底的回避风险的办法。

2.3.5 风险跟踪

风险跟踪是负责监视和缓解风险的人员获得、编辑和汇报风险状态信息的过程，检查风险的对策是否有效，为主动风险控制提供依据。

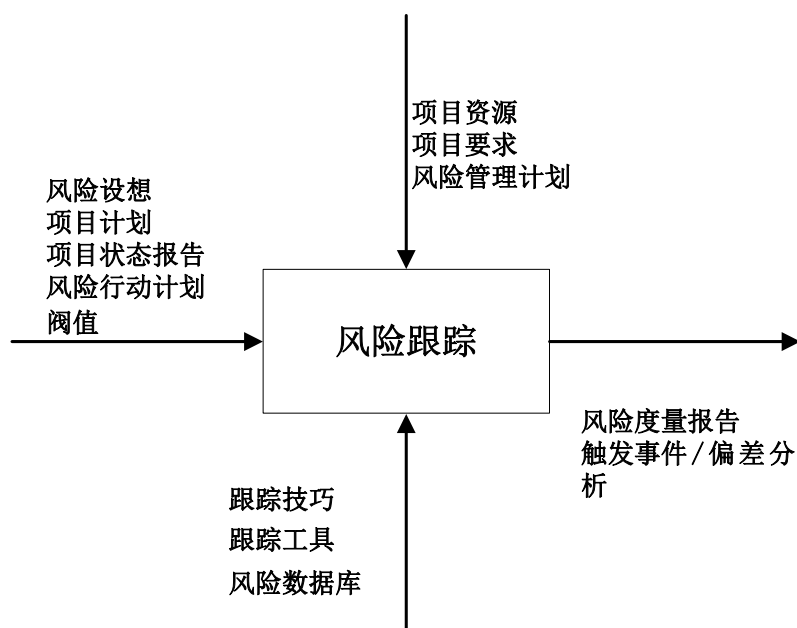


图 2-6 风险跟踪过程定义

（资料来源：本研究整理）

如图 2-6 所示的是一般风险跟踪过程的定义。一般风险跟踪过程的定义包括位于顶部的控制调节过程，包括企业的资源，风险管理计划等；底部的机制支持过程，包括风险跟踪技巧，风险跟踪工具和企业风险数据库；左边的输入是风险跟踪进入过程，包括软件外包企业的经营状况和相关数据，当前的风险状态等；右边是系统输出的结果，主要输出的是风险的度量和风险审计结果，触发器和相关的风险分析结果。风险跟踪可以通过风险审计，偏差分析和企业相关指标分析等方法进行有效的风险跟踪。风险审计，项目风险管理部门应定期进行风险审核，进行事件跟踪和主要风险因素跟踪，以进行新风险的再评估。偏差分析，在项目中，项目组应定期与基准计划比较，分析成本和时间上的偏差。企业相关指标分析，技术指标分析主要包括项目相关指标（如项目进度，质

量，成本等指标）和其他企业自身密切关注的指标。技术指标分析将比较原定技术指标和实际技术指标差异。

风险跟踪包括监控处于潜伏期和活动期的所有风险。对可能触发风险的各个因素进行监控，通过对各项风险指标的综合评价确定风险发生可能性的变化趋势。若显示风险发生可能性的迹象增加，则风险有逐步演变为现实的可能。风险跟踪过程包括监视风险状态以及发出通知启动风险应对行动。

这些方法的核心就是定义企业项目管理的底线，也就是通过定义触发器，一旦风险相关的分析超过底线，触发器就引发相关的风险报警信息。

2.3.6 风险控制

风险控制是项目经理分析跟踪风险报告中的数据、制定风险决策并实施的过程，执行风险管理过程，确保项目团队在整个项目生命周期内一直保持风险意识。

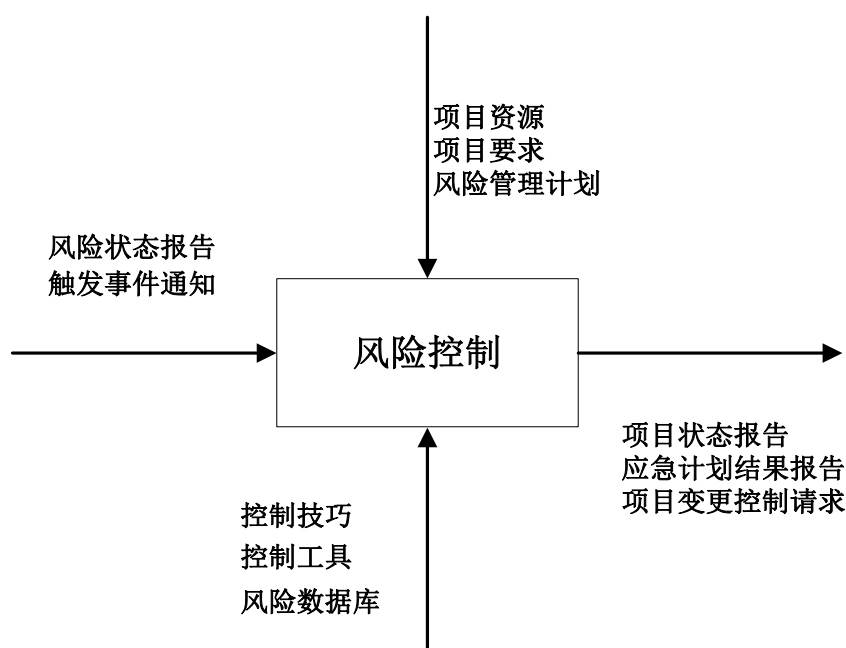


图 2-7 风险控制过程

（资料来源：本研究整理）

风险伴随着项目执行的整个过程，风险的出现会增加项目的费用，减缓项目的进度，并对项目的完成质量产生很大的影响，从而影响投资者的预期收益。主要的风险控制活动如下：

（1）分析

分析风险数据包括检查风险数据的趋势、偏差及异常情况，目的是了解当前每一风

险状态，及时制定有关的缓解计划。

（2） 决定

决策需要借助风险数据库，决定下一步进行风险管理的方法，一般有以下几种与风险决策：重新计划、关闭风险、使用应急方案继续跟踪风险并执行当前风险计划。

（3） 执行

执行单个的风险管理计划包括根据定义的里程碑来监测风险，并做出有关风险及其应对战略的决策。

2.3.7 风险数据库

利用信息技术建立风险管理数据库。由于风险来源于信息的不对称，所以建立起良好的风险管理数据库就成为风险管理活动的前提和基础。风险管理每个阶段产生的文档和数据都要进行规范的管理。各类数据、知识、经验都需要归档记录。如果没有使用风险数据库，风险管理的效果就有可能达不到 IT 项目的要求，并且可能导致项目失败，从而使风险管理没有意义。风险数据库除了及时记录风险管理过程中的各种信息，为本项目的风险管理提供必要的信息，还可以为其他项目风险管理提供借鉴，是企业风险管理的知识库。根据每个项目的差异性，风险管理数据库可以独立于 IT 项目，风险数据库也可以是 IT 项目数据库其中一部分。

2.4 本章小结

本章首先对中小金融公司的项目风险特点进行了概述，进而结合项目特点提出了项目全面风险管理和全生命周期风险管理理念，可以为软件项目的风险管理提供参考和借鉴。然后对该模型框架的风险管理过程组五大风险管理过程进行了详细的论述。

第三章 F 公司软件风险管理

在前面章节，我们对金融行业的软件项目特点以及全面风险管理理论，风险管理过程等进行了系统地分析，在接下来的内容中将以 F 公司的软件项目实施过程为例，对中小金融业软件项目的风险管理理论的应用进行详细分析论证。

3.0 F 公司及项目概况

F 公司是广东省内首家汽车金融有限公司，为国内的汽车终端消费者及汽车销售商提供金融服务的非银行金融机构，主营业务是为其母公司旗下相关品牌的汽车终端客户和经销商提供汽车金融服务。信息技术与金融业务高度融合已成为金融业打造核心竞争力的重要手段，公司的业务开展已高度依赖于 IT 系统。

在实施金融软件项目时，不仅需要了解业务，熟悉流程，还需要在用户需求完整的情况下充分考虑到各种风险，以及极端情况下的应对方式。

从公司成立开始，引入汽车零售信贷业务系统(NETSOL)，库存业务审批系统，资金管理系统，总账系统，数据仓库平台，并将这些系统作为核心业务平台，其他的所有系统称为外围系统，项目实施通常以核心业务系统为中心，外围系统可直接与核心系统通信，也可通过中间代理系统与核心系统通信。系统之间的通信都必须有严格的报文规制，明确的握手次数和严密的加密信息。

由于金融业务的复杂性和金融机构的多样性，在业务系统方面，基本是定制化开发为主。总结 F 公司软件项目的特点，具体有如下几方面：

(1) 业务相关：软件项目无论是核心业务系统还是外围系统，都与业务紧密相关，与业务流程紧密结合。所有的业务流程，都是由相应的业务部门提出，都有业务需求。

(2) 管理规范：F 公司有严格的规范，这些规范包括很多，如项目规范，文档规范，流程规范，设计规范，开发规范，编码规范，测试规范，项目结束标准等。在项目过程中，无论源系统有什么样的要求，必须要按照项目相应的规范去执行，输出相应的文档。

(3) 组织复杂：在 F 公司内部所有的项目，都是隶属于 IT 部，但提出需求的是相应的业务部门。由于业务部门比较多，导致在信息交流，需求沟通等方面需要与更多的干系人联系，使看上去简单的沟通变的复杂。

(4) 团队协作：在项目执行过程中我们会与不同的人进行沟通，在需求阶段，需

要和业务部门的客户进行需求沟通；在开发阶段，需要和外包供应商，用户进行不断的成果确认。由于项目自身的特点，不断需要和其他的业务系统进行数据交换；在测试阶段，需要和外部的测试团队进行测试工作。因此，只有项目团队和其他团队相互支持和合作，才能圆满完成项目。

（5） 成果确定：项目结束后输出的成果，不仅是项目组完成的项目。还包括公司规范所规定的一些成果，比如源代码，设计文档，原型图，操作手册，验收报告等。项目验收的成果，不仅仅是 IT 部门方面，还包含相应的业务部门。

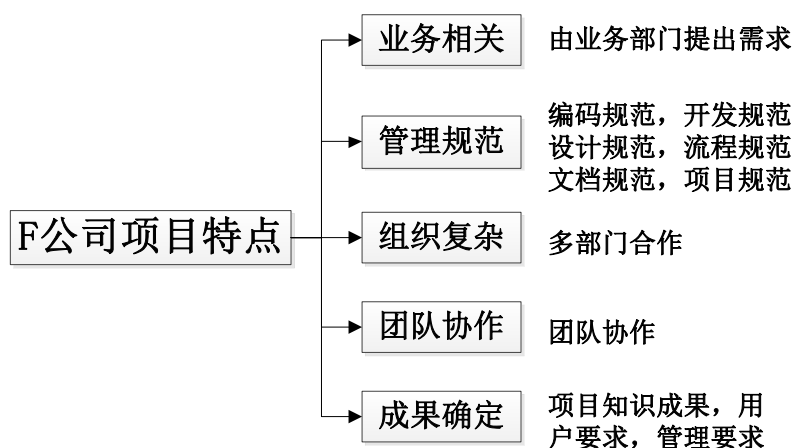


图 3-1 F 公司项目特点

（资料来源：本研究整理）

从 F 公司项目的特点可以看出，金融软件项目管理和其他项目的差别并不是很大，都是需要经过需求分析，设计开发，系统测试和上线实施等流程。只是比其他项目安全性要求更高，各个系统的协调配合度高，对项目进度控制要求严格，必须遵守业务流程规范等。更明显的特点是：项目内负责人比较多。既有公司内部的项目经理，技术经理，业务分析师，还有外包公司的项目经理，技术经理等。另外汇报的干系人也比较多，分别向 PMO 办公室，IT 部和业务部门以不同的形式和内容进行汇报。

由于 F 公司软件项目的复杂性，为了确保项目顺利开展，确保项目顺利实施，由 IT 部门牵头与持续控制部门一起负责构建了全面风险管理体系，在风险管理体系建设，项目管理计划制定，风险识别过程，风险控制策略方面做了全面的规划部署。

3.1 构建全面风险管理体系

随着金融创新业务的开展对 IT 系统也提出了更高的要求。信息化既是促进金融创新、推动金融业发展的一个重要支撑手段，也是管理和防范风险、保障金融稳定的重要

工具。因此，信息系统的稳定是确保公司业务正常开展的重要保障。然而系统风险的防范，要使用先进的方法论和工具，须做到精细化的风险管理，这就对服务商的资质、综合能力以及信息系统建设和运维管理提出了更高的要求^[10]。F 公司为确保 IT 项目顺利完成，建立了 IT 项目全面风险管理体系，该体系主要包括风险管理环境，风险管理制度设定，风险监测与识别，风险评估，风险定价与处置，内部控制，风险信息处理和报告，风险持续改进，各模块具体内容如下：

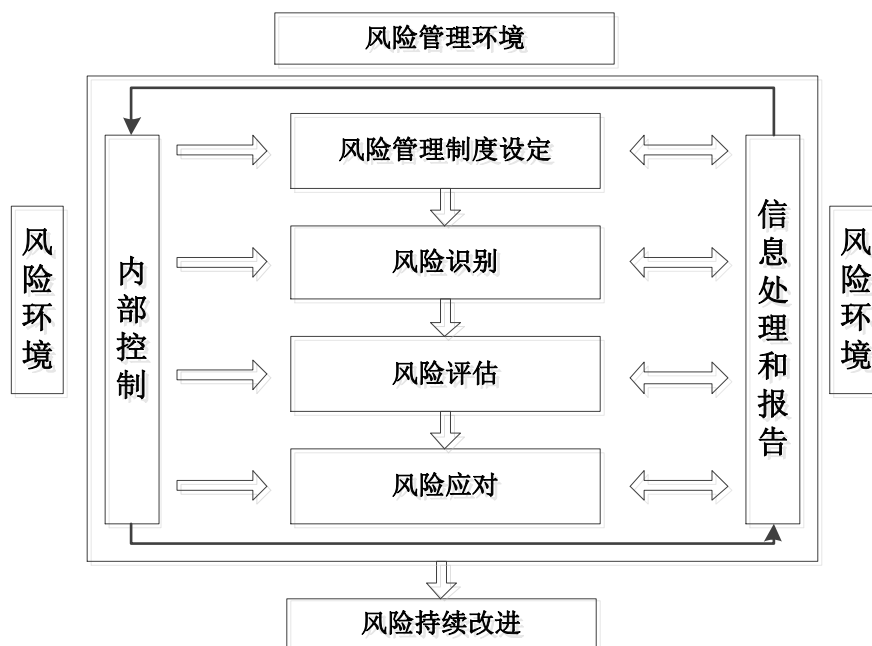


图 3-2 全面风险管理体系

(资料来源：浅析企业全面风险管理与 IT 项目风险管理的关系 2009 年全国项目管理教育论文集)

(1) 风险管理环境：风险管理环境主要包括内部环境和外部环境。建立风险管理环境是进行全面风险管理的基础。具体包括风险管理文化建设，项目管理制度，矩阵组织架构等。其中风险管理文化是全面风险管理的核心，关系到全体员工对项目风险管理的重视程度，直接影响项目目标的实现，项目风险识别和分析，风险应对策略等多方面问题；矩阵式组织架构是项目管理的组织保障，也是实施全面风险管理的支撑。

(2) 风险管理制度设定：需要为风险管理设定一套可执行的管理制度，IT 项目要将风险管理贯穿于项目管理每个阶段，通过设定每个阶段风险偏好和风险容忍度，制定明确的风险管理制度，主要明确风险管理的工作流程、风险管理报告的内容，并针对常规性的风险管理工作制定具体的报告模板。

(3) 风险监测与识别：在项目开始后，监测项目的进展和项目环境是否变化，行业发展状况，核对项目风险管理策略和措施的实施效果是否与风险计划一致。执行风险管理过程以应对风险事件。寻找机会改善和细化项目风险应对计划。获取反馈数据，确保未来的决策更加符合实际。

(4) 风险评估：风险评估可分为定性分析和定量分析，量化风险事故带来的影响和损失的程度，并按潜在的危险大小进行优先排序。从内部和外部两个方面来进行风险评估过程：外部视角详细说明过程输入，机制，控制和输出；内部视角详细说明用机制将输入变成输出的过程活动。

(5) 风险定价：对每一种情况都要有具体的定价策略。好的定价估算是在现有的信息基础上反复思考后的决策。有些估算是成本关系估算，有些则是使用成本模型。在进行定价估算前要收集启动估算过程所要用的信息，类似项目的最新经验，专业的参考材料，市场和行业调查，有关运营和过程的知识，使用估算软件和数据库，与行业专家访谈。

(6) 内部控制：持续控制部门配合内控部门建立一套健全的内控制度实施操作风险控制流程，及时发现项目实施过程中存在的问题，提出和实施改进方案。对操作风险进行事前防范，事中控制，事后监控，确保项目的顺利实施。

(7) 风险信息处理和报告：利用风险管理软件帮助处理风险管理数据，把输入系统的各种形式的原始数据分类，整理录入数据库存储，以供查询风险因素，对风险源进行风险识别，判断，并进行分析评估，为全面风险管理提供决策依据以回避风险。但是风险管理不可以过分依赖于软件系统，要建立科学的风险汇报制度，对各种风险管理执行的效果进行总结，定期向管理层汇报项目风险状况。

(8) 风险持续改进：基于 PDCA 循环的系统化的风险改进方法。风险持续改进需要观察每个阶段的整体改进效果。首先要识别项目风险流程改进的机会，评价需要改进的风险流程，分析项目实施过程中存在的问题，实施风险流程改进，评估风险流程改进的效果并积累风险改进的经验。同时，持续控制部门应根据公司内外部环境，银监会对操作风险的监管要求，及时发现风险改进过程中发现的问题，对风险管理制度和风险管理流程中存在的问题提出修改和调整意见，上报公司决策层来对全面风险管理体系进行持续改进。^[17]

3.2 风险管理体系建设

在组织结构上，确立董事会、高管层、信息技术委员会负责信息科技风险战略和政策制定、治理结构建立、资源配置等工作，明确 IT 风险管理机构在全行风险管理组织体系中的定位，明确各业务模块、各业务支持保障部门、各级机构的 IT 风险管理职责，并参照国际先进银行做法，构建了信息技术管理部门、风险管理部门、各前台业务条线、各中后台业务支持保障部门、各级机构必须充分参与的公司 IT 风险管理的“三道防线”；在政策层面，将信息科技风险纳入公司风险管理政策及风险偏好；在流程方面，明确信息技术管理部门作为 IT 风险管理的主要执行者，向部门领导和首席风险官实行双线汇报，定期开展信息科技事件案例分析，指导完善政策制度，推动管理流程改进和重要问题解决，从组织、政策、流程方面切实将信息科技风险纳入全面风险管理框架。

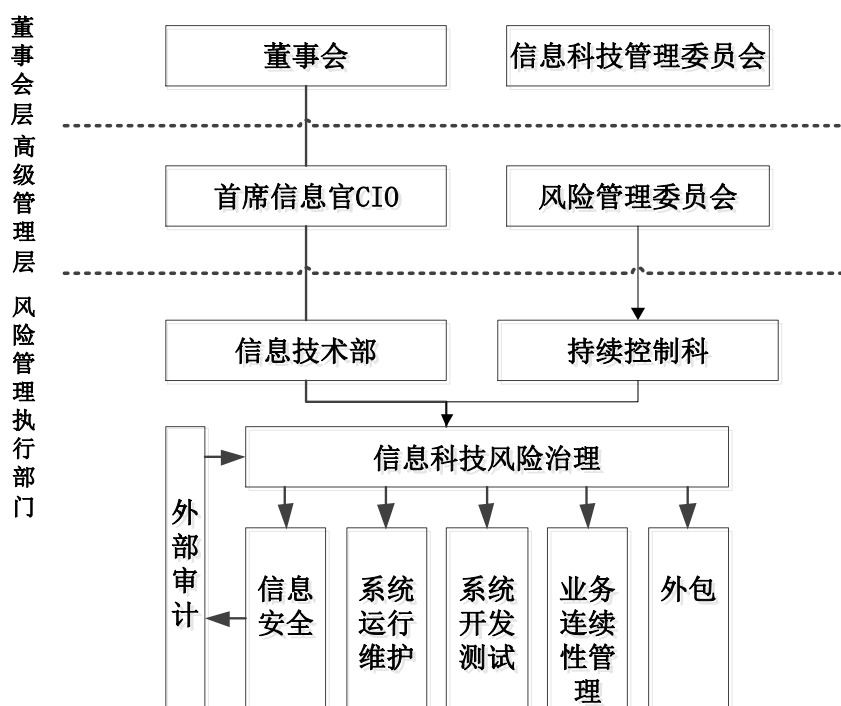


图 3-3 F 公司信息科技风险管理体系结构图

（资料来源：本研究整理）

第一．F 公司的董事会肩负信息科技管理职责：

（1）审查并批准公司信息化管理战略，保证与公司的总体发展战略相一致，评估 IT 管理水平和对业务部门的支持能力。监控信息科技风险和安全事故的发生；

（2）对于关键的信息安全风险给予重点关注，并对风险管理提出指导意见，确保公司的风险管理策略与监管部门的要求一致；

(3) 设立信息科技管理委员会，主要来自高级管理层，外部咨询公司专家，IT 部门领导和主要业务部门的代表，负责监督信息系统操作风险，审核各项风险管理制度，定期向高管汇报 IT 系统操作风险政策的执行情况，IT 项目的运作情况和 IT 部门风险管理的整体状况；

第二. F 公司设立首席信息官 (CIO)，向公司高管汇报 IT 的管理状况，参与 IT 政策的执行，首席信息官的职责包括：

(1) 负责信息科技战略，尤其是软件系统开发策略，符合公司的总体业务战略和信息科技风险管理策略；

(2) 负责信息科技部的建设，承担并履行公司的 IT 部门领导职责，负责 IT 系统建设预算和支出，IT 部门管理制度建设，IT 工作流程建设和改善，负责 IT 内控制度设计，IT 系统开发和实施，IT 项目立项和管理，系统和基础设施的建设运行，系统维护和升级，信息安全管理，灾难恢复管理，外包商合作管理等职责；

(3) 确保有效的 IT 系统风险管理，并使有关管理政策措施在公司每个部门得到执行；

(4) 负责 IT 部门其他科技风险管理工作；

第三. 信息科技部门直接负责 IT 项目的风险管理和 IT 系统的操作风险监控，风险管理的范围涵盖了软件项目，系统安全，系统操作风险，业务连续性管理等方面。

第四. 公司设立持续控制科负责 IT 系统和公司业务持续开展管理工作，并直接向首席信息官和公司高管汇报工作；该部门负责协调 IT 系统风险政策的制定和操作风险的监控，特别是 IT 信息安全，业务连续性控制和合规操作风险等方面，持续控制部门给出具体的指导意见，并对用户或者 IT 技术人员使用 IT 系统提出合规方面的要求，进行 IT 系统安全评估，对风险改进效果进行评估，负责监控高层对 IT 系统风险管理改进意见的落实，监控信息安全威胁和突发事件的发生。

从风险管理体系可见，公司对 IT 风险管理十分的重视。设立持续控制科协助 IT 项目的风险管理工作，从高层到各执行部门自上而下的职能组织结构，使得公司 IT 项目的风险管理更为直接，有助于快速发现并汇报重大风险，并协助做出决策，从而有利于对公司 IT 项目的风险控制。

3.3 项目风险管理计划

项目风险管理计划就是在项目正式启动或者启动初期，对项目风险的一个统筹考虑，

项目规划的过程。主要目的是尽快消除风险，制定若干备选行动方案，建立时间和经费储备以应对不可避免的风险。主要考虑的问题有两个：风险管理策略是否正确？实施的管理策略和手段是否符合项目总目标？因此项目风险管理计划主要包括下面两方面工作：管理层针对项目面临的风险制定行动方案，选择适合于选定行动路线的风险规避策略^[23]。

风险管理计划的目的是确保正确确定、分析、记录、减轻、监测并控制项目风险。它说明将要用于确定、分析、按优先级排列、监测和减轻风险的方法。如果风险或减轻风险的策略有变更，则应该更新风险管理计划。

在风险管理计划的基础上进行风险跟踪和风险控制，一旦发现风险的可能会发生，就要采取预先设定的合理措施进行风险控制。

项目风险管理计划的制定：

（1）确定风险管理的过程与工具

首先要确定风险管理遵循的过程，以便确定风险、分析风险、确定风险优先级。还需要确定记录和存储风险数据时使用的工具或技术。

（2）创建风险初始化列表

了解将要处理的风险种类之后，才能制定风险管理策略。在项目早期阶段创建一个风险初始列表，并以此指导后续风险管理过程。创建风险列表应遵循的原则，确定并评估风险中说明的过程。

（3）指定风险管理团队

F 公司非常重视风险专家团队的建设，IRM 团队成员并非由专门从事风险管理工作的员工组成。相反，团队成员已在公司拥有一份全职工作，他们只是暂时承担风险管理任务。有必要时候获得高级管理层的支持，从而对资源进行合理的分配。任何团队都需要一名领袖，IRM 团队也不例外。公司挑选持续控制部门经理来管理这个团队，使用 50%~70%的时间来处理项目风险管理工作。

（4）确定十大风险的应对策略

风险管理团队需要对风险清单上的所有风险都应确定具体的应对方法，时刻监控风险是否发生；还应准备好应急计划（补救措施），以备风险发生的时候及时应对。风险应对方法包括积极风险应对，消极风险应对（减轻、预防、转移、回避、接受）。

（5）确定十大风险的风险指标

风险清单中的每项风险定义量化指标,如果该指标出现,则表明风险随时可能会出现。这些条件即风险指标。项目经理在项目实施期间监测这些风险指标,并实施风险管理计划中的应急方案。

(6) 定期进行风险报告和复审

只有在项目进行过程中持续进行风险管理,定期进行风险检查和报告,风险管理才会有成效。风险管理计划中包含定期报告风险状态和召开风险复审会议的计划表,还需要计划定期召开风险复审会议的前提条件。

风险计划随着项目状况的变化而变化,在项目开展过程中不断进行更新。在任何项目中,风险管理都需要作为一个日常活动列入项目管理计划,是项目管理人员的一项重要工作。

3.4 项目风险识别过程

软件项目整体可划分为八个阶段:调研,立项,需求,设计,编码,测试,实施和维护。在项目风险管理的风险识别阶段,软件项目沿用了金融业现有的风险识别方式^[7]:

(1) 明确风险识别的目标

依据全生命周期管理理论和项目管理规划,项目发起人和项目经理要一起确定风险管理的范围和重点,并且确定本阶段风险识别的主要目标。IT 项目处在不同生命周期阶段,项目风险管理都有不同的重点关注方面,风险识别也会各有不同,并且风险识别着重关注本阶段中的主要风险源。

(2) 明确项目主要干系人

确定本阶段的主要项目干系人,项目组成员及分工等。项目经理不仅要熟悉项目的内容,也要了解项目组成员情况,包括项目管理人员、系统开发技术人员以及能为项目风险识别提供信息的用户。项目经理挑选的项目成员最好具有业务和技术方面的综合知识,了解项目的目标及面临的风险。项目组成员需要善于沟通和具有团队合作精神,要乐于分享信息,拓展团队成员的业务知识,扩展个人和团队的知识面。

(3) 收集资料

项目风险识别需要收集的资料包括 IT 系统或项目说明书,事业环境因素,组织过程资产,项目范围说明书等。其中产品或项目说明书可以从项目章程、项目合同中得到,也可以参考需求说明书总结得出。事业环境因素和组织过程资产可以从项目章程或者项目管理计划得到。识别 IT 项目风险的重要手段之一借鉴过去类似项目的经验和教训,

通常可以查看项目风险数据库、阅读公开出版的书籍、期刊杂志等资料和访谈项目参与者获得类似的信息。

(4) 确定风险识别的技术与工具

通常的风险识别技术与工具有德尔菲法、头脑风暴法、SWOT 分析法、检查表、因果分析图、系统或过程的流程图、影响图、WBS 法、经验判断法、试验法等。风险识别过程在项目的全声明周期内的每阶段都会循环发生。

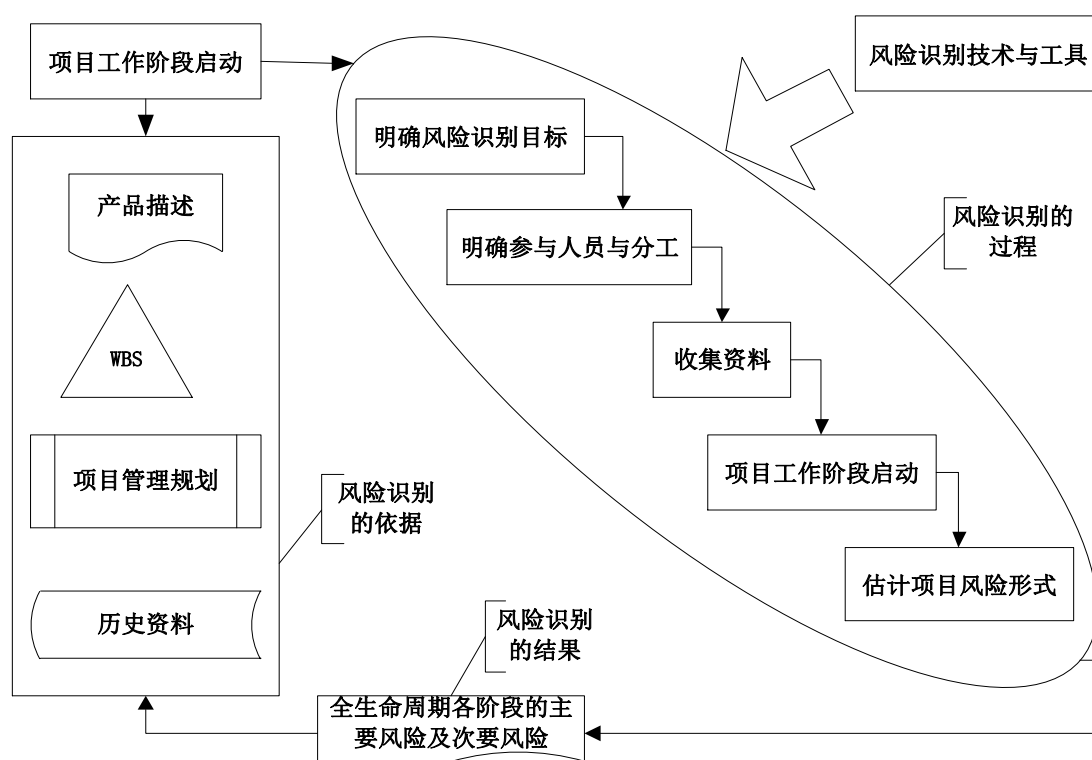


图 3-4 全生命周期风险识别过程

（资料来源：王寓辰，张金隆，卢新元，陈艳．全生命周期下 IT 项目风险识别研究．管理学报，2005 年第 9 期）

各项目阶段的面临主要风险、次要风险对项目开影响程度差异性比较大，在各阶段都要分别重点关注（表 3-1）。

表 3-1 软件项目生命周期各阶段主要风险与次要风险表

项目周期	内容	参与部门	工作职责	主要风险	次要风险
调研	项目需求方整理需求, 调研	公司业务部	公司业务部根据市场状况, 为满足业务需求, 整理系统需求	需求风险	
立项	项目需求方提出立项申请, 项目管理方立项审批	公司业务部, 信息技术部, PMO 办公室	公司业务部提出立项申请, 由公司管理层批准立项, PMO 办公室全程跟踪项目情况	立项风险、技术风险和计划风险	协调风险、组织人才风险、责任心风险和政策环境风险
需求	项目需求方进行需求细化, 开发方完成需求分析, 功能分析	公司业务部, 信息技术部	终端用户和业务分析师共同细化需求, 开发人员协助完成功能分析。	需求风险, 资源风险, 系统规模风险和进度风险	人力资源风险、协调风险、责任心风险、稳定性风险和经济风险
设计	项目开发方进行系统设计	公司业务部, 外包公司, 信息技术部	外包公司基于现有核心业务系统, 在考虑兼容性基础上, 完成系统设计	管理风险, 相关性风险和进度风险	协调风险、人力资源风险、责任心风险和稳定性风险
编码	外包公司完成系统编码, 代码检查	外包公司, 信息技术部	外包公司完成编码, 代码检查; 公司业务部配合进行需求功能细化	技术风险, 进度风险	协调风险、人力资源风险、责任心风险、系统稳定性风险
测试	信息技术部完成功能测试, 压力测试	信息技术部, 公司业务部	组织完成功能测试, 压力测试, 公司业务部配合完成功能测试案例	技术风险, 相关性风险	协调风险、保障性风险、人力资源风险、责任心风险

表 3-1 软件项目生命周期各阶段主要风险与次要风险表(续)

项目周期	内容	参与部门	工作职责	主要风险	次要风险
实施	运维部门制定上线计划，完成系统上线	外包公司，信息技术部，公司业务部	运维部门制定系统实施计划，数据迁移方案，外包公司配合实施，公司业务部配合完成业务验证	计划风险、技术风险、进度风险、合作风险，资源风险，管理风险	协调风险、保障性风险、人力资源风险、责任心风险
维护	运维部门进行系统日常维护	信息技术部，公司业务部	运维部门进行系统日常运维工作，故障处理；与外包公司，公司业务部配合系统推广	需求风险，资源风险，系统规模风险	协调风险、保障性风险、责任心风险、系统稳定性风险
收尾	信息技术部关闭项目	信息技术部，外包公司，业务部门	信息技术部总结项目经验，负责项目收尾，业务部门配合项目关闭	费用风险	保障性风险

(资料来源：本研究整理)

软件项目风险识别的过程灵活运用风险识别方法，对项目整个实施过程进行风险识别，保证项目风险识别的有效性，全面性。

3.5 项目风险控制策略

(1) 建立全面风险管理文化。全面风险管理文化建设需要公司全体员工的积极参与、支持和坚持不懈地努力。要在广大员工心目中，牢固树立“风险无处不在，风险无时不有”、“控制风险就是创造效益”的观念，努力营造全面风险管理的舆论氛围，最终形成具有本公司特色的风险管理文化。分析确认企业的风险体系，梳理管理过程中各流程、环节的风险点，系统地进行归类整理；倡导鲜明的风险管理的理念，明确风险管理文化的价值观，如违规损失永远大于冒险利益；制订完善的规章制度，确立各项相关的工作流程。

(2) 做好培训机制和加强交流学习。开展各种风险管理培训，宣传风险管理理念，使员工掌握风险管理技能，营造全面风险管理氛围。风险存在于项目周期中的每个阶段，控制风险，更多的是公司管理水平问题，要提高公司风险管理水平就需要做好培训和知识共享交流工作。

(3) 建立项目信息披露制度。在公司内部大力提倡风险披露制度,加强部门之间、项目组之间、员工之间、领导与员工之间的交流沟通,开设风险管理知识、项目经验、制度规范、典型案例、经验分享等栏目,筛选一些典型的风险案例刊登在公司布告栏中,提供给公司所有员工学习、讨论,提高大家识别风险、防范风险的能力。

(4) 着重风险的事前预防。在项目风险控制过程中,树立正确的风险防范意识,将风险关注的时点前移,把各种风险在萌芽状态消除掉,避免通过事后补救来解决。在项目过程中,各种风险的前兆都会以某种形势表现出来的,如果是没有及时发现,马上纠正或者对出现的问题麻痹大意,容易将风险错误扩大化,形成损失,为此需要付出高昂代价。因此,进行早期风险预警才比较理想,事后控制不如事中控制,事中控制不如事前预防。

总之,IT 项目的风险管理,并不能仅仅靠某一项技术手段管理方法就可以解决,应需要多种技术和管理方法的整合应用,健全和优化风险管理的制度,丰富发展公司的风险管理文化,从各个层次,对各种类型的风险进行全面管理,从全面风险管理体系的角度看,首先建立企业风险管理文化,改善内部风险管理环境;二是设定明确的风险管理目标和政策;三是建立完善的风险识别和监控系统;四是不断提高风险评估技术水平;五是逐步完善风险应对策略,建立风险数据库;六是由持续控制部门牵头,建立完善的内部控制体系;七是建立风险信息报告机制;最后要建立风险管理持续改善机制。

3.6 本章小结

本章介绍了 F 公司的基本概况与 IT 项目概况,以及 F 公司建设全面风险管理体系、项目风险管理计划、风险识别与控制策略等内容。从中可以了解 F 公司进行风险管理的模式与现状,也可以看出 F 公司在项目风险管理方面具有很好的企业重视度,这为有效地开展项目风险管理提供的有力的支持。下面章节将着重分析 F 公司软件项目关键的风险因素之间的关系并提出具体的规避措施。

第四章 基于 ISM 模型的风险分析

通过对 F 公司软件项目的现状分析,建立了全面风险管理体系,主要包括风险制度建设,风险计划制定,风险识别和控制策略等。接下来本章针对 F 公司 IT 项目在风险管理活动中存在的风险问题,在项目风险识别的基础上,运用系统工程的解释解构模型法(Interpretative Structural Modeling)^[27],建立 IT 项目全过程风险结构模型,并通过模型分析,对 F 公司 IT 项目风险管理提出具体的实施建议。

4.1 项目主要风险

国内外很多学者对 IT 项目风险管理,风险识别方法,风险评估技术做了很多研究。但是都是按照项目阶段分步进行研究,并且是对单个的项目风险进行识别和风险分析,对项目各阶段产生的风险联系、各个风险的层次关系缺乏关注,并且对风险的整体结构研究甚少。实际上掌握不同的风险之间的关系,对风险管理非常重要,通常一个风险会导致另外的几个风险事故的发生,如果控制好这个根源风险,那么其他风险就可以投入比较少的人力物力,这样风险管理能起到事半功倍的效果。

与普通 IT 项目相比,金融软件项目具有流程更长,安全性要求高,项目实施过程更为复杂的特点。结合巴塞尔银行监理委员会提出的十大金融服务风险类别,对项目开展过程中,遇到的各种主要风险进行总结和深入分析后,从风险类型、风险描述、发生概率、影响程度、处理方式等方面对 F 公司 IT 项目风险进行了总结整理,确定项目面临的主要风险用表格的方式归纳如下:

表 4-1 金融机构 IT 项目风险列表

序号	风险类型	风险描述	发生概率	影响程度	处理方式
1	外包决策风险	公司高层选择外包供应商决策失误	低	大	避免
2	供应商选择失误	对供应商的核心能力和过程能力评价不准确所造成的对供应商的选择失误	低	大	避免
3	需求分析不准确	对业务部门提交需求进行可行性分析不够深入,导致出现偏差	高	大	避免
4	需求变更风险	由于业务部门提出的需求不明确造成需求不断变更,甚至项目范围扩大	高	大	避免
5	设计方案出现偏差	在设计方案中,使用的实现方法不当,功能设计出现错误,功能设计考虑不周全,造成系统处理错误	中	大	避免

表 4-1 金融机构 IT 项目风险列表(续)

序号	风险类型	风险描述	发生概率	影响程度	处理方式
6	里程碑失控	监控计划缺陷，公司对监控环节不重视所造成的监控失控	高	中	控制
7	缺少用户支持	用户积极配合项目开展对项目成功至关重要，需要职能部门经理授权执行项目执行	中	中	控制
8	评价标准不准确	在项目合同中，对项目验收的标准，测试计划，提交的项目交付成果等等评审标准不一致	低	低	避免
9	软件开发达不到要求	由于技术水平，人员能力，资源条件或责任心不足所造成的结果，系统出现一些功能或影响安全运行的错误	中	大	控制
10	用户过高期望	项目上线后功能不能满足用户的需要，达不到用户的期望，导致期望与现实差距过大	中	大	减轻
11	售后服务风险	技术支持人员不到位，分析问题、解决问题不及时等	中	大	避免
12	文档风险	文档内容描写不符合规定，描写不清楚	中	中	避免
13	沟通风险	发包方，供应商的协同工作机制不能发挥正常作用	中	中	控制
14	合同风险	由于合同签订的合同缺陷及合同类型错误选择导致出现技术和资金上的纠纷	低	中	避免
15	人力资源风险	人员流动特别是技术骨干力量流失。	中	大	控制
16	进度风险	由于项目范围不断扩大或者人员安排等导致的项目延期，不能到期完成项目的问题	高	中	控制
17	费用风险	超过项目预期费用	中	中	控制
18	外包风险	主要是项目开发过程中，外包商出现问题，造成项目中断。对外包商的依赖性强，更换外包商的成本高	低	大	预防
19	团队管理风险	主要是制度建设、流程建设、协调控制、应急管理等方面不完善造成的团队工作问题	高	大	预防
20	政治法律风险	不同国家政治体制，法律环境不同，不同公司之间企业文化，管理制度差异造成的人员，技术，法律法规意识等方面的问题	低	中	避免

(资料来源：本研究整理)

4.2 项目全过程风险识别

针对 IT 软件项目运行过程中涉及到的多种风险,在公司内部对内控风险管理团队和项目团队 16 位专家进行咨询与调查,其中包括项目经理、开发人员、测试人员、业务人员、软件开发及内控管理人员、QA 等。根据所设定的问题,设计第 1 份问卷,见附录一。问卷中列出 20 余项风险因素清单。然后采用德尔菲法(Delphi)请专家采用问卷的形式进行调查再分析,按照变异系数的计算方法分别对调查对象的评分结果进行统计分析,将各位专家的意见分析归纳总结,将最后一轮总结后的意见集中,最终的得到 10 项主要风险因素清单。

表 4-2 项目风险因素清单

风险因素	因素	权重	描述
需求分析不准确	S1	4.31	需求内容表述不清,导致需求容易发生变化,技术人员对需求内容理解错误,需求分析出现错误等
供应商选择失误	S2	4.25	对供应商的核心能力和过程能力评价不准确所造成的对供应商的选择失误
需求变更风险	S3	4.25	由于业务部门提出的需求不明确造成需求不断变更,甚至项目范围扩大,成本上升,进度延迟
外包决策风险	S4	4.19	公司高层选择外包供应商决策失误
缺少用户支持	S5	4	用户积极配合项目开展对项目成功至关重要,需要职能部门经理授权执行项目执行
里程碑失控	S6	3.88	监控计划缺陷,公司对监控环节不重视所造成的监控失控
设计方案出现偏差	S7	3.81	设计方案、功能设计出现错误,功能设计考虑不周全,变更计划不周全,使用新技术风险。
沟通风险	S8	3.75	发包方,供应商的协同工作机制不能发挥正常作用
人力资源风险	S9	3.69	人员流动特别是技术骨干力量流失。
进度风险	S10	3.63	由于项目范围不断扩大或者人员安排等导致的项目延期,不能到期完成项目的问题

(资料来源:本研究整理)

4.3 建立构思模型

设计第 2 份问卷,采用 DEPHI 法进行问卷调查,见附录二。专家对该表中的风险因素之间的关系作进一步分析后,给出各个风险因素之间的关系,通过调查表进行多次迭代和统计分析,得到因果关系结果如图所示,表中“▲”代表横向因素对纵向因素有影

响，空格表示没有影响。由此得到项目风险因素构思模型。

表 4-3 调查结果表

		0	1	2	3	4	5	6	7	8	9	10
		项目 风险	需求 分析 不准 确	供应 商选 择失 误	需求 变更 风险	外包 决策 风险	缺少 用户 支持	里程 碑失 控	设计 方案 出现 偏差	沟通 风险	人力 资源 风险	合同 风险
0	项目风险	▲										
1	需求分析不准确	▲	▲		▲			▲				▲
2	供应商选择失误	▲	▲	▲	▲	▲	▲	▲	▲			▲
3	需求变更风险	▲			▲			▲				
4	外包决策风险	▲				▲		▲				▲
5	缺少用户支持	▲			▲		▲	▲				▲
6	里程碑失控	▲						▲				
7	设计方案出现偏差	▲						▲	▲			▲
8	沟通风险	▲	▲		▲	▲	▲	▲	▲	▲		▲
9	人力资源风险	▲	▲		▲			▲	▲		▲	▲
10	进度风险	▲										▲

(资料来源：本研究整理)

在上述基础上，建立邻接矩阵：

$$M = [M_{ij}] = \begin{matrix} & \begin{matrix} S0 \\ S1 \\ S2 \\ S3 \\ S4 \\ S5 \\ S6 \\ S7 \\ S8 \\ S9 \\ S10 \end{matrix} \\ \begin{matrix} S0 \\ S1 \\ S2 \\ S3 \\ S4 \\ S5 \\ S6 \\ S7 \\ S8 \\ S9 \\ S10 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{matrix}$$

图 4-1 邻接矩阵

(资料来源：本研究整理)

根据软件计算结果，可以得出如下可达矩阵和骨架矩阵：

-----Reachable Matrix-----										
1	5								10	
1	0	1	0	0	1	0	0	0	1	1
1	1	1	1	1	1	1	0	0	1	2
0	0	1	0	0	1	0	0	0	0	3
0	0	0	1	0	1	0	0	0	1	4
0	0	1	0	1	1	0	0	0	1	5
0	0	0	0	0	1	0	0	0	0	6
0	0	0	0	0	1	1	0	0	1	7
1	0	1	1	1	1	1	1	0	1	8
1	0	1	0	0	1	1	0	1	1	9
0	0	0	0	0	0	0	0	0	1	10

图 4-2 可达矩阵

（资料来源：本研究整理）

-----Skeleton Matrix-----										
1	5								10	
0	0	1	0	0	0	0	0	0	1	1
1	0	0	1	1	0	1	0	0	0	2
0	0	0	0	0	1	0	0	0	0	3
0	0	0	0	0	1	0	0	0	1	4
0	0	1	0	0	0	0	0	0	1	5
0	0	0	0	0	0	0	0	0	0	6
0	0	0	0	0	1	0	0	0	1	7
1	0	0	1	1	0	1	0	0	0	8
1	0	0	0	0	0	1	0	0	0	9
0	0	0	0	0	0	0	0	0	0	10

图 4-3 骨架矩阵

（资料来源：本研究整理）

4.4 建立重排序的可达矩阵

根据级间划分的结果可以得到重排序后的可达矩阵 M'

$$M' = \begin{matrix} & \begin{matrix} L1 \\ L2 \\ L3 \\ L4 \end{matrix} & \begin{matrix} S0 \\ S3 \\ S6 \\ S10 \\ S1 \\ S4 \\ S5 \\ S7 \\ S2 \\ S8 \\ S9 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \end{matrix}$$

图 4-4 重排序的可达矩阵

(资料来源：本研究整理)

根据重排序的可达矩阵 M' 建立风险因素结构模型，如图 4-5 所示。

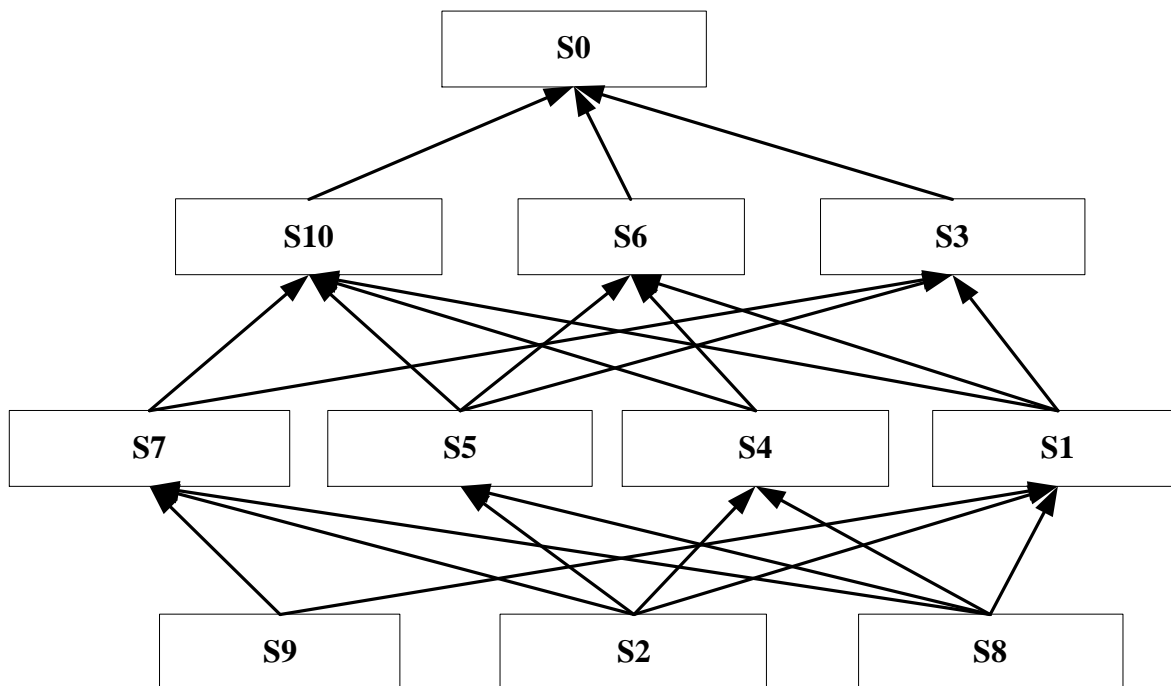


图 4-5 风险结构模型

(资料来源：本研究整理)

从图中看出，该模型是一个四级递阶的有向层次结构模型，自下而上的箭线表示下一层因素影响高一层因素。

4.5 建立解释结构模型

根据上述结构模型，建立解释结构模型，如图所示：

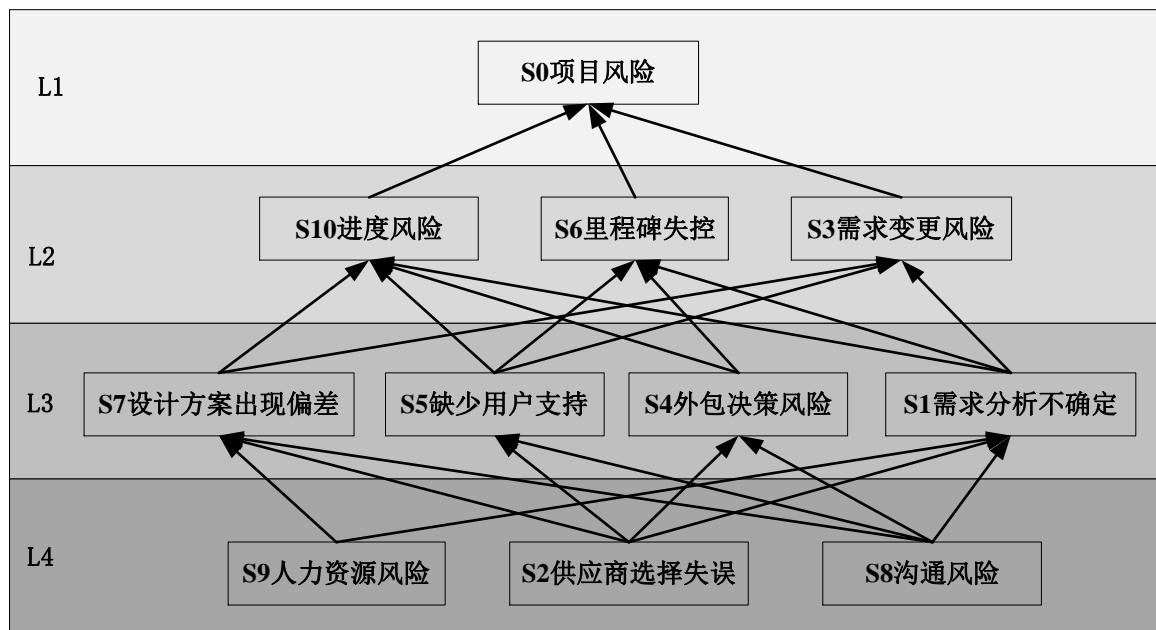


图 4-6 解释结构模型

（资料来源：本研究整理）

4.6 解释结构模型分析

通过对 F 公司软件项目各风险因素的风险解析模型进行分析，总结出对于项目风险的根源由一个具有四级递阶的层次结构的因素体系组成。具体分析如下。

（1）最底层有人力资源风险、供应商选择失误、沟通风险等 3 个主要的风险因素。它们是影响项目是否成功的关键因素，特别是供应商选择失误风险出现在项目运作的早期阶段，会影响项目过程中双方合作是否顺利开展，对项目是否成功影响非常大，应该进行重点关注。

（2）第 2 层是影响项目成败的直接风险因素，包括进度风险、里程碑失控和需求变更风险 3 项。这 3 项风险间接受到多种风险因素的影响，最终影响项目的顺利实行，且此 3 项风险产生影响重大直接影响到项目的成败。

（3）项目需求分析不确定、设计方案偏差、缺少用户支持、外包决策失误风险等多项风险，是导致项目进度风险，里程碑失控等风险的直接原因，在项目开展过程中需要重点监控。

（4）项目进度风险主要来自设计方案偏差、缺少用户支持，需求分析不确定风险，

外包决策风险，这些因素都会直接导致项目延期，不能及时满足业务需求。更深层次的原因在于缺乏有效的沟通，前期供应商的选择有失误，没有全方位考核供应商的技术人力和管理水平，并且项目组人力资源变动，技术和业务水平都更不上。

通过这样的解析模型非常直观的分析，IT 项目风险之间的关系比较明确，高层管理者可以有选择性的进行相关风险的预防措施，风险管理部门也可以更有效的发挥他们的作用，及时对风险进行监控。

4.7 对项目风险管理的一些建议

通过对 F 公司软件项目各种风险因素的评估和分析，把风险发生的概率、损失严重程度综合起来考虑，可得出在软件项目实施过程中发生各种风险影响程度和项目成功的机率，从而决定应采取什么样的措施规避风险。在某种程度上，项目组需要及时进行风险应对，认真的执行，快速的反应，灵活的调度和沟通，因此平常的风险应对的培训必不可少。

利用风险解释结构模型对项目风险进行分析后发现，在项目风险管理过程中需要注意以下几个问题：

(1) 需求分析不准确与需求不断变更互为因果关系，需求不明确引起需求不断变更，需求不断变更也会造成需求分析不准确。用户过度期望与需求分析不准确也存在类似的关系。需求风险对项目产生各种影响，项目风险管理人员必须在早期进行重点预防，加强需求沟通，业务分析师需要在项目前期全新投入工作，尽量明确每一项需求的内容、范围、要求。

(2) 对项目部分外包的决策与选择问题。应充分考虑和分析项目部分外包的可行性和成本分析。在项目开展过程中外包商主要承担系统设计和代码开发工作，直接影响项目的质量和系统能否成功上线，在进行供应商选择的时候，要对外包商的技术和管理水平、公司组织结构、行业经验、售后技术服务水平等方面严格考核，防止由于外包商选择失误所带来的各种风险。

(3) 进度风险控制。项目进度缓慢会影响项目的成本，如果项目导致系统上线延迟，可能影响业务开展，还可能造成系统质量问题。进度控制的目标是了解项目的当前状态，了解导致进度变更的因素。确定进度是否已经发生变更，以及当前发生变更时，管理好这些变更。控制项目进度的变更首先要确保所编制的项目进度符合时机，要使用纪律手段来控制项目的进度，并且要由领导来强调按照进度开展项目的重要性。虽然许

多工具和技术可以帮助进行进度控制，但是项目经理需要格外重视人事管理问题。项目失败不是业务编制的 PERT 不好，而是因为人事管理的失败。

(4) 交流与沟通。与用户的需求沟通、与外包商的合作沟通都将对项目产生重大的影响。只有双方建立良好的沟通与协作机制，才能努力完成项目的目标，只有建立有效的项目信任沟通机制，才能避免在需求分析、系统设计、系统评价标准、项目验收标准、项目质量等方面可能出现的分歧与失误。实施软件项目是外包双方互相配合、共同合作的过程。

4.8 本章小结

本章首先针对项目开展过程中所存在的多种风险，对公司 10 位专家进行咨询与调查，设计问卷，总结软件项目主要风险清单。再经过多次迭代统计分析，得出项目风险因素构思模型。运用布尔代数法则对邻接矩阵进行运算，获得可达矩阵。再对可达矩阵进行级间划分和重排序，得到风险结构模型与解释结构模型。在对解释结构模型进行分析后，对项目风险管理提出具体的建议。

第五章 F 公司软件项目关键风险规避与对策

通过上一章的 ISM 模型分析,总结了项目各风险间的因果关系,并且对每项风险的规避措施给出了具体建议,本章综合前面分析的十大项目风险因素,归纳出影响项目正常运行的 5 类关键风险如下:需求分析风险、项目沟通风险、项目进度风险、设计方案风险、项目合作风险。本章对这五类关键风险进行详细的描述和剖析,并提出具体的规避措施。

5.1 需求分析风险

5.1.1 风险描述

需求分析阶段业务分析师对用户提出的需求理解不透彻,对用户的要求把握不准,在形成需求分析稳定的时候容易描述不清,引起业务流程理解错误风险,导致项目开发过程中出现需求分析错误,容易引起需求变更等风险。需求分析风险是项目风险的关键风险,在项目分析阶段需要对需求分析导致的风险进行重点管理和预防。

需求分析风险还表现在项目无法跟着业务的变化。因为业务变化就有可能改变最初的项目需求分析乃至项目规划。随着公司金融创新不断,业务变化频繁。这种变化会使得 IT 项目变得越来越复杂,如果开发人员不能适应这种变化,将会导致 IT 项目的失败。

造成需求分析风险的原因是多种多样的,比如业务部门人员岗位变动、前期项目遗留问题未决、业务管理流程没有定型等等。在实施软件项目过程中遇到的典型的需求风险问题,进行总结归纳,得到以下三个主要方面。

(1) 关键用户不能参与需求分析

通常用户参与就是某位高层把自己的想法含糊不清地传递给基层员工,然后由该员工代表领导参加需求分析会议。如果提出需求的高层工作太忙,总是不能亲自参加需求细节的讨论,那么项目组就不能准确的把握用户的真实需求。

(2) 项目需求蔓延

在项目范围定义得到批准之后,由于项目的功能和特征不断的微量增加。这些小的需求既耗费时间又浪费资源。比如项目发起人可能会提出在项目范围中增加一些花里胡哨的功能,导致需求越来越多。有时候项目范围扩大并不总是由项目发起人引起的,也可能是项目组内部发生的范围蔓延。有些成员有些新奇的想法想要加到项目中。项目团队对这些新奇想法的过分热情会分散他们对项目初期需求的注意力。导致对用户的需求

理解错误。

（3）业务需求跳跃

系统功能和特征发生明显改变，比如业务部门初期想实现为客户提供某项新产品和服务，如果此基础上增加另外的一个新的业务功能，那么需求就出现了跳跃，会导致项目 MOV 变化，这时候项目组织需要考虑现在项目的价值。

5.1.2 规避措施

可以通过采取一些必要措施将需求风险尽可能降低至可接受的水平。针对上面谈到的典型需求风险，我们可考虑从以下几个方面入手实施风险规避。

（1）对需求变更的控制

在软件项目实施中出现需求变更是非常正常的，并且随着业务的不断发展，部分需求变更也合理，项目组需要全力支持。对控制需求变更的措施首先是要降低需求变更的频率，尽量减少需求变更对项目的不良影响。实施需求变更控制通常会采取以下几种措施。

1) 规范项目需求变更流程，由需求部门领导和业务分析师共同组成需求评审组，对需求定义和需求变更进行严格评审，增加提出需求变更的难度，目的让用户理解需求变更容易导致项目范围扩大或者项目延期，进而影响系统上线；

2) 需求确定后，要有明确的需求变更标准，业务分析师及时提供需求分析文档，以正式文件的形式发到业务部门，在用户签字确认后，再将需求提交项目组开发人员进行需求分析，是要求业务部门对需求确认工作给予必要的重视；

3) 需求变更不可避免，要业务人员首先确认需求变更的优先级别。在保证项目早期的核心需求不受影响的情况下，采取分批分步的步骤逐步实现；

4) 在与业务人员的交流中注意沟通技巧，对业务人员提出的变更需求尽量通过各种方式给予巧妙地引导，比如向用户推荐其他可行的方案来对提出的需求变更进行思维转化。

（2）对需求质量的控制

对需求质量控制关键是要找到关键用户进行需求调研。通过前面的分析可以看出，需求调研对象的岗位、个人经验和对业务的熟悉程度都会直接影响需求分析的全面性、有效性和合理性。由于信息系统面向的是各个层面的使用者，因此在确定需求调研对象时应首先将需求按使用户按照不同级别进行分类，针对不同的需求选择最熟悉业务流程

的用户来访谈。同时针对不同类型的调研对象，应注意采取适合的访谈方式，并在提问时给予必要的引导。例如在访谈管理者时，他们通常会提供一些比较原则性的、抽象的、方向目标一类的需求信息，而对要实现的具体功能考虑不足。而对于操作人员来说，他们往往非常直接提出非常具体的细节化的需求，缺乏对目的和整体体系的描述，使需求收集人员看不清方向。这就要求访谈人员根据这些特点向被访谈者提出引导性的、有针对性的问题，启发他们对忽略的需求点做出考虑，这样才能保证收集到的需求信息是完整的。

（3）需求理解差异的控制

由于业务人员和技术人员的专业背景和工作领域不同，容易对需求的理解出现偏差，这也是导致项目返工和项目效果达不到用户要求的重要因素。要尽可能减小误差，就需要双方在进行需求调研时沟通尽可能充分。特别是业务分析师，在进行需求调研时要主动发问，对于不清晰的功能需求要反复确认，直到双方理解准确无误为止，撰写的需求文档要清晰明了。在讨论需求时，可以尽量要求业务人员举例说明需求，并在需求文档中详细记录案例内容。此外，针对不同业务模块，可指定业务部门熟悉业务的用户全程参与需求分析的过程，BA 可以随时找关键用户进行需求沟通，消除技术人员的需求理解误解。

5.2 项目沟通风险

5.2.1 风险描述

项目缺乏沟通将导致业务用户、IT 开发人员和外包商的技术团队不能充分发挥团队合作的优势。

（1）用户与需求分析师的沟通

需求分析师主要职责就是收集用户的需求，如果业务分析师不能深入用户部门了解用户的真实需求，提供的需求文档出现偏差，会影响项目需求分析的效果和后期项目上线维护工作顺利开展。

（2）业务分析师与外包商沟通

供应商和 IT 部沟通不畅是对项目是否能顺利开展起关键性的作用。外包开发人员获取需求的渠道就是业务分析师，如果业务分析师和技术人员沟通不畅，导致项目成果并不是业务用户真实的需求，直接影响项目的交付质量。

5.2.2 规避措施

保持良好的沟通渠道，使项目各方都可以及时准确地掌握业务真实需求、项目进展情况以及项目团队可能遇到的技术难题，对于金融企业开发软件项目过程中涉及到多部门合作是有重要的意义。为了确保项目沟通顺畅，可以采取下面的风险控制方法：

(1) 制定详细周密的项目沟通计划，对于沟通计划中的内容，需要根据项目组成员的职责和权限不同，有不同的版本。确保计划能够保密，又能最大限度地帮助到所有的项目成员。项目沟通计划会根据干系人的变化随时更新，增加或者减少干系人，更新干系人的沟通方式，沟通内容等等。

(2) 项目团队随时采用各种的沟通渠道（比如电子邮件、多方电话、面对面交谈、类似 QQ 等即时通讯工具），与项目干系人保持紧密的联系。

(3) 定期召开项目团队每周会议，比如项目状态评审会，解决问题会议和技术设计评审会议等。项目状态评审会议主要目的是通知情况，明确问题和建议行动细则。解决问题会议是在项目出现问题时及时召开会议，技术设计评审会议是在设计阶段对系统设计进行评审，保证系统的可用性和稳定。

(4) 在项目的需求分析阶段，项目分析师可以采用调查问卷的方式收集用户的需求，让用户及时将问卷发回给项目团队，以便使项目团队尽可能清晰地掌握业务部门的实际要求，从而尽早了解项目需求并清楚项目的难点。

(5) 由于金融系统项目的开发具有独特的个性，并且业内没有通用的开发模式，一般情况下，业务分析师应该及时为项目团队提供支持。当遇到难以解决的问题时，为了沟通响应时间，项目技术人员可以直接与用户进行沟通交流，直接获取用户的需求和想法。

在所有沟通方式当中，面对面的沟通是最有效的沟通方式。直接告知和展示要比写出来以后让其他人更容易看到效果。更重要的是，别人会通过面对面接触了解你的初衷，让你的信息更容易被表达，意图更容易被理解。

5.3 项目进度风险

5.3.1 风险描述

软件项目的实施是一个相对长的过程，过程中进行进度风险控制，保证项目里程碑按时完成，是确保项目计划顺利的重要保证，对项目的成败至关重要。虽然在项目开始

制定了分阶段的进度计划，在实施过程中进度计划可能受到内外部等多种因素的影响，按项目计划实现项目阶段性成果存在困难，造成项目无限期延长。

进度风险带来的影响：如果项目不能按照计划完成阶段任务，项目成员承受的压力比较打，甚至对项目管理失去信心，影响项目目标的实现。项目延期也会导致项目干系人对项目不满意，可能会导致业务不能正常开展，给公司造成损失。

5.3.2 规避措施

（1）建立项目实施联络机制，根据项目涉及应用范围大小，组织关键业务人员和技术人员参加。加强培训学习，提高技术支持人员处理问题，解决问题的能力。

（2）建立项目实施工作流程，确保项目相关的人员按时完成所负责的领域。加强项目进度的控制，项目进度控制的主要依据是项目进度计划表，定期检测项目成员的工作成果和遇到的困难，并及时协调解决问题，确保项目里程碑的达到。

（3）在需求评审与分析的时候，不指定项目人员具体负责那一块，而是要求项目组成员对本项目所有需求都要有所理解，并能够理解项目中的任意一个需求。在确认每个团队成员理解本项目所要实现的所有需求之后，项目经理才让团队成员对相应的开发任务进行确认，具体落实到人。采用这种方式，使得每个项目成员对本项目的所有需求都有所理解。在人事变更（比如原先负责某个需求的人员请假或者离职）时，可以快速得找到能够承接任务的人，进而规避了进度风险。

（4）制定项目实施过程中，出现问题的应急预案。项目成员在遇到问题时，通过个人的努力超过 30 分钟以上而仍然未能将问题解决时，要及时寻求团队成员的帮助，而不是继续在问题上打转，耽误项目时间。

（5）由于某些项目周期较长，项目成员往往在漫长的开发过程中看不到自己的工作成果，会逐渐失去工作热情。因此，在项目过程中及时展示项目组成果（比如通过项目状态板展示已完成项目成果），对团队成员来说也是一种精神激励。



图 5-1 项目状态板

(资料来源：本研究整理)

5.4 设计方案风险

5.4.1 风险描述

设计方案风险主要是指对用户需求理解不准确、进行系统设计考虑不周全，购买的软硬件性能不能满足业务发展的要求等技术方面问题，导致项目设计方案存在风险，主要包括以下几个方面：

(1) 方案完整性风险：即由于项目功能需求分析不到位导致的风险。这种风险通常与用户界面的设计、数据处理程序、灾难恢复程序、数据保护机制及信息安全措施等有关；

(2) 方案变更风险：由于需求分析不准确，在项目进展过程中用户不断提出需求变更导致设计方案不断进行变更的风险。主要与用户需求确定，需求变更控制和项目范围控制有关；

(3) 数据安全风险：即系统数据或业务信息存储不当而导致的风险，影响数据或信息的可获取的难易程度。在 BS 结构的系统应用广泛，数据安全风险是企业面临的主要威胁之一。存储风险主要与业务程序的确立、数据管理控制、应用系统的安全、数据处理环境、计算和网络安全等有关；主要与数据处理过程的监控、备份和应急计划、数据恢复技术等有关；

(4) 体系结构风险：即系统结构规划不合理或者不能满足业务需求所带来的风险。

主要与信息技术架构是否健全、软件技术资源配置、IT 系统安全的设计和运行、网络操作环境、数据管理相互之间统一性等有关；

（5）其它相关风险：即其他影响企业业务开展的设计风险。主要是 IT 系统对业务持续开展的支持、风险预警系统、业务中断及恢复等有关；

5.4.2 规避措施

（1）成立评审委员会，做好每一个设计方案的评审工作，找出方案设计、功能设计等方面存在的问题。对于项目组设计好的功能说明书，要提交给提出需求的业务部门进行审定，方案评审完毕请需求部门填写需求确认书。建立变更管理机制，及时处理项目开发过程中出现的一些需求变更问题。

（2）规划和设计好与不同应用之间的接口规范。如果项目涉及到系统之间数据传输，上线后将影响现有系统的正常运行，是影响整个项目成果的关键之一。项目组可以成立专家小组，进行专题讨论，提出切实可行的数据接口方案，并对方案进行严格的论证。对于技术难关，可以成立攻关小组，攻克技术难题。做好技术人员的培训，加强新技术的学习，了解业内行业发展的最新进展，提高设计人员设计水平。

（3）按照系统工程的思路和方法，结合管理信息系统原理，在系统结构框架保持稳定的情况下，按一定的标准和规范，分阶段分步骤开发业务系统，比如将项目分成多期进行，在前一期项目完成后系统稳定并且满足业务要求的情况下再进行下一期系统的实施。IT 部门要对系统的建设进行整体规划，并设定一定的技术标准，这样做不但能够确保当前项目的成功实施，保证各系统之间数据交换稳定。而且能减少项目失败风险，对整体 IT 系统建设进行很好的把控。

5.5 项目合作风险

5.5.1 风险描述

合作风险是指项目实施过程中存在公司各部门合作及与外包供应商合作的风险。一是项目团队内部、各部门之间合作的风险；二是公司与外包商在项目实施期间所发生的风险。

由于金融系统的复杂性，在系统开发过程中设计到的系统比较多，涉及的部门也很多，各个部门之间配合协作，共同完成项目目标非常重要。如何协调部门之间的工作，让用户积极参与到项目当中，合理安排干系人的工作，避免工作出现扯皮，获得职能部

门经理的支持，甚至是公司高管的支持都是非常重要的问题。

另外将软件项目外包在节省 IT 管理成本的同时，也带来了外包风险。主要包括：

- (1) 由于过分依赖供应商，公司对项目质量和项目资源的把控有限；
- (2) 由于公司不能对核心的技术进行把控，不能够在系统架构上甚至技术方案的选择方面做出单方面的决策，获得供应商提供的服务也差强人意；
- (3) 由于业务水平的限制，供应商对公司的业务流程和金融系统的运作不能充分理解，开发的系统也会存在隐藏的质量问题；
- (4) 供应商在现场实施项目服务，公司的信息安全受到威胁。因此，在项目实施过程中，公司需要着重关注信息安全管理，加强外包商安全风险管理工作；

5.5.2 规避措施

虽然选择合适的外包供应商可以降低企业的成本，降低部分风险，但是本公司和外包公司的管理制度和企业文化不同，增加了项目外包过程的合作风险。为了规避这些风险，IT 部门需要与供应商之间建立良好的合作机制，IT 部门需要确保对项目实施过程有决策和控制权。双方要建立彼此信任，共同合作的氛围。

(1) 项目经理需要加强领导和管理的力度，尤其是在沟通和协调各部门工作管理中应该投入更大的精力，要在这方面多想一些主意，打造一个成员都认同的项目团队。同时也要求项目组全体成员配合和支持项目经理的工作。

(2) 建立外包公司资源档案，需要对供应商进行全方位评价，不仅要看外包商的技术能力，而且要对该公司的财务能力、资信等级等整体能力进行评估，确认供应商有非常好的技术水平和稳定的合作能力，双方合作过程中要定期进行适当的评价和报告。

(3) 项目团队内部要做好沟通工作，强化团队建设，在项目实施的过程中要主动与供应商进行沟通。IT 部应与外包服务商建立有效的日常联络沟通和信息交流机制。

(4) 外包商技术人进场进行项目开发前，IT 部门需要按照公司的持续控制制度对外包人员进行相关制度的培训。

(5) 在项目环境发生变更时，IT 部门应该评估该变更对供应商的服务带来的影响，并提供相应的方案，保证环境变更期间项目的顺利开展。环境的变更包括公司组织结构和领导职位的变更，还有供应商的人员变更等，公司内部组织的变更对项目的影响，由持续控制科去进行评估并给出解决方案。外包商组织发生变更，项目经理需要及时评估影响，并调整项目的计划方案。

(6) 在系统开发过程中, 采取相应的防范机制, 确保项目合作过程中信息安全管理符合公司相关安全和审计规章制度。持续控制科需要定期对外包商在项目期间的操作风险进行评估, 对发生的事故和故障进行处理处理并跟踪, 保证信息安全。

(7) 系统正式上线运行后, IT 部门应与外包服务商建立有效的联络机制, 确保项目结束, 外包商撤离现场, 还能及时对系统提供必要的技术支持。

5.6 本章小结

本章重点讨论了 F 公司在风险管理过程中出现的关键风险, 包括与外包商的项目合作风险, 项目沟通风险, 项目进度风险, 项目需求风险, 设计方案风险等。并针对这些风险, 提出了相应的规避措施。

结 论

软件项目的高成功率与其全面、细致、严谨的项目风险管理是分不开的。项目通常在立项、开发、实施、维护等各个阶段都存在不同程度的可变因素，从而在整个生命周期中都随时伴随着风险。现代项目的特点与现状要求风险管理必须是全方位、全生命周期的管理。项目的全生命周期管理，是对项目从其需求立项到项目收尾的全过程进行宏观的统筹管理。

通过对 F 公司实施 IT 项目涉及的各种风险进行深入的分析和研究，在全生命周期风险管理模型的基础上，结合全生命周期等理论和本人在 F 公司多年的从业经验，使用 ISM 解释结构模型对项目风险进行了深入研究分析。并提出面向 F 公司项目风险管理的全面风险管理模型。该模型包括风险管理目标与政策设定、风险检测与识别、风险评估与控制、风险信息处理与报告、持续的风险管理等几个部分。另外对于中小金融机构，仅有风险管理模型是不足以让他们安全面对风险，还需要探讨了如何正确实施风险管理的问题。本文以 F 公司软件项目为研究对象说明 F 公司应该如何应用本文提出的风险管理模型，如何建立相应的机制，如何使用 ISM 模型对软件项目面临的风险进行关系分析，如何应对项目风险，并为如何解决这些风险提出本文的解决方案。

本文的创新之处在于构建出面向中小金融公司的全生命周期风险管理模型。

(1) 在 F 公司 IT 项目风险管理案例分析的基础上，引入全生命周期和持续风险管理，提出了面向中小金融机构的 IT 项目风险管理模型。将风险管理过程由分块管理变成全面风险管理，项目过程中对风险管理进行持续控制并及时更新风险管理计划，由被动变为主动。

(2) 使用 ISM 解释结构模型分析 F 公司项目风险之间的层级关系，分析得出 F 公司软件项目的风险解释结构，总结出最需要关注的根源风险和直接风险。并针对性地提出了风险管理建议。

(3) 针对 F 公司软件项目实施过程中，存在许多风险问题，本文分析了几个关键风险，对风险产生的原因进行了分析，并且对如何避免这些风险提出了具体的规避措施。

虽然本文在风险管理方面提出了较为创新的风险管理模型，但由于资源和时间等各方面的限制，本文也存在一些缺陷之处。

(1) 本文主要是研究 F 公司的软件项目风险管理，虽然研究的案例也具有代表性，但是只研究本公司面临的主要风险，研究样本数量不是非常多，文章研究提出来的风险

管理模型在实际项目管理中应用的效果，还需要更多的同行业软件项目的成功案例的支持。

(2) 在 F 公司软件项目的风险管理体系中，所采用风险模型侧重通过对风险清单进行风险的识别、分析，并采取应对策略。在此建议在风险管理过程中适当引入相应的工具、技术进一步风险量化，可以更直接，有效地评估风险，使得风险管理方案的选择，风险应对策略的使用提供了更有力量化的数据、理论依据。

(3) 不同的管理水平与文化背景的公司，在进行项目风险管理时，在风险管理的策略和关注的内容都有非常大的差异。因此，在构建 IT 项目全面风险管理体系时，要根据各家公司的管理实际情况和项目的运作水平进行认真分析之后，提出有针对性的解决方案。

本文对风险因素识别和风险之间的层级关系进行了研究。根本目的是为了能够制定合理的风险分析和控制策略，从而有效的进行风险管理。通过 F 公司 IT 项目风险因素的识别、风险间的关系等相关研究，发现 F 公司在实行 IT 项目风险管理的过程中，存在各种不确定风险因素，都会对项目造成消极影响，虽然在项目管理过程中采取控制措施，但是还是有意外风险事故发生。在今后的风险管理研究中，主要围绕企业全面风险管理文化建设，风险持续控制进行研究。首先是扩大研究范围和研究样本数量，关注同行业之间软件项目的风险因素分析，从而得到行业内项目管理风险因素的全面了解。其次，着重风险分析方法和控制措施的研究，从而进一步完善风险管理模型。

参考文献

- [1] 王友乾. 金融 IT 项目的风险识别方法[J]. 中国金融电脑, 2009: 41-42
- [2] 卢有杰. 现代项目管理学[M]. 北京: 首都经济贸易大学出版社, 2004: 30-31
- [3] 沈建民. 项目风险管理[M]. 北京: 机械工业出版社, 2003, 20
- [4] 邱莞华. 现代项目风险管理方法与实践[M]. 北京: 科学出版社, 2003, 11
- [5] 张亚莉, 杨乃定, 杨召君. 项目的全寿命周期风险管理研究[J]. 科学管理研究, 2004, (2) : 27-30
- [6] 方德英, 李敏强. IT 项目风险管理理论体系构建[J]. 合肥工业大学学报(自然科学版), 2003, 26(S1): 907-911
- [7] 王寓辰, 张金隆, 卢新元, 陈艳. 全生命周期下 IT 项目风险识别研究[J]. 管理学报, 2005, (9) : 5-9
- [8] 赵恒峰, 邱莞华, 黄斌江. 风险间关系的研究及其在风险管理中的应用[J]. 科研管理, 1996, (17): 24-29
- [9] 杨乃定. 企业风险管理发展的新趋势[J]. 中国软科学, 2002 , (6) : 54-57
- [10] 钱巍. 浅析企业全面风险管理与 IT 项目风险管理的关系[J]. 2009 年全国项目管理教育论文集: 113-115
- [11] 冯春山, 吴家春, 蒋馥. 项目中主要风险的管理[J]. 预测, 2002, (6): 67-69
- [12] 贾晓霞, 杨乃定, 姜继娇. 项目区域风险的模糊综合评价方法研究[J]. 工业工程与管理, 2004, (1): 4-8
- [13] 吉迎东. 基于全生命周期的 IT 项目风险管理策略模型分析[J]. 山西财经大学学报, 2006, (4) : 92
- [14] 赵恒峰, 邱莞华, 王新哲. 风险因子的模糊综合评判法[J]. 系统工程理论与实践, 1997, (7) : 93-96
- [15] 梁小勇, 陈宪. 项目生命周期模式的确定[J]. 技术经济, 2004, (04) : 58-59
- [16] 杜伟, 毛剑波. 基于项目全寿命周期的风险管理研究[J]. 技术与市场, 2005, (05) : 52-53
- [17] 黄映辉. 项目管理: 基于生命周期和基于职能活动的管理[J]. 郑州轻工业学院学报(社会科学版) , 2004, (2) : 26-29
- [18] 林鸣, 沈玲, 马士华, 陈健华. 基于全寿命周期的项目成功标准的系统思考[J]. 工

- 业工程与管理, 2005, (01) : 101-105
- [19] 朱启超, 陈英武, 匡兴华. 现代技术项目风险管理研究的理论热点与展望[J]. 科学管理研究, 2005, (04) : 41-45
- [20] 周智海. 风险管理的新趋势:风险自留[J]. 北京工商大学学报(社会科学版), 2002, (01) : 40-43
- [21] 杨志刚. IT 项目实施中的风险管理[J]. 露天采矿技术, 2009, (02) : 69-72
- [22] 高维义, 彭华涛. 积极风险回避与消极风险回避的比较分析[J]. 价值工程, 2005, (03) : 110-111
- [23] 谢彬. IT 项目风险管理理论与实践[D]. 西安: 西南交通大学, 2003
- [24] 徐姝, 胡明铭, 李自如. 风险矩阵方法在业务外包风险评估中的运用[J]. 管理现代化, 2004, (02) : 13-16
- [25] 万江平, 杨建梅, 刘尚余. 系统工程能力成熟度模型的研究[J]. 计算机应用研究, 2001, (07) : 49-51
- [26] 李金昌, 黄劲松. 风险理论发展的比较分析[J]. 经济学家, 2006, (2) : 125-128
- [27] 章文杰, 解武杰. ISM 模型在风险结构分析中的应用[J]. 商业研究, 2002, (02) : 1-3
- [28] 肖春明. 浅谈中小银行软件外包中的项目管理[J]. 华南金融电脑, 2008, 11: 89-91
- [29] 张莉. IT 软件项目风险管理三维结构研究[J]. 煤炭技术, 2010, (4) : 238-241
- [30] 方德英, 寇纪淞, 李萍, 秦立. IT 项目风险管理保障体系设计[J]. 商业研究, 2006, (10) : 51-54
- [31] 商瑞强. IT 项目风险管理分析[J]. 计算机工程应用技术, 2010, (6) : 154
- [32] 陈建斌, 武刚, 路梅, 方德英, 王海燕. IT 项目风险管理关键成功因素实证分析[J]. 安徽农业科学, 2010, (3) : 1518-1520
- [33] 王寓辰, 张金隆, 丛国栋. 基于粗糙集的 IT 项目风险评价方法研究[J]. 工业工程与管理, 2006, (2) : 87-91
- [34] 杨俊明. 浅析中小软件项目开发的风险管理[J]. 福建电脑, 2009, (2) : 52
- [35] 莫湘群. 软件项目的进度风险管理[J]. 电脑与信息技术, 2002, (4) : 67-70
- [36] 曹青, 董纪昌, 佟仁城. 中小银行 IT 外包的风险分析和策略[J]. 管理评论, 2005, (10) : 24-28
- [37] 王晓军. 中小银行如何做好 IT 风险管理[J]. 中国金融电脑, 2009, (9) : 17-19

- [38] 王燕. 以全面风险管理策略应对商业银行 IT 风险管理面临的新挑战[J]. 中国金融电脑, 2012. (7): 25-28
- [39] 张成虎, 李淑彪. 信息技术风险监管_银行监管的新领域[J]. 中国金融电脑, 2002, (9): 20-23
- [40] 钱峰. 适应信息化建设的商业银行信息科技风险管理策略[J]. 现代管理科学, 2012, (2) : 33-35
- [41] 郭英见. 银行 IT 外包及其风险管理策略[J]. 中国金融电脑, 2006, (1) : 30-33
- [42] 陆媛. 国有商业银行技术风险控制测度模型研究[J]. 中国管理信息化, 2008, (9) : 66-69
- [43] 郝亮. 金融行业的 IT 项目管理[J]. 现代商贸工业, 2009, (1) : 212-213
- [44] 郝继升. 浅谈软件项目风险管理[J]. 延安大学学报(自然科学版) , 2009, (04) : 27-30
- [45] 钱巍. 企业全面风险管理理论在 IT 项目风险管理中的应用[D]. 上海: 上海交通大学, 2009
- [46] 任雪利. 基于 UML 的软件风险控制的研究与系统开发[D]. 西安: 西安理工大学, 2006
- [47] 王羽. 商业银行软件项目风险管理研究[D]. 北京: 北京邮电大学, 2008
- [48] 张珞玲, 李师贤. 软件项目风险管理方法比较和研究[J]. 计算机工程, 2003, (03) : 91-94
- [49] Project Management Institute . A Guide to the Project Management Body of Knowledge(Fourth Edition) [M], 2008
- [50] Kathy Schwalbe . Information Technology Project Management(5th Edition) [M]. Cengage Learning, 2007
- [51] Johanna Rothman . Manage It , Your Guide to Modern , Pragmatic Project Management[M], 2007, 6
- [52] Harold Kerzner, Ph . D. PROJECT MANAGEMENT A Systems Approach to Planning, Scheduling, and Controlling(10th Edition) [M]. John Wiley & Sons, Inc. , Hoboken, New Jersey, 2009
- [53] Brooks F P. The Mythical Man-month [M]. Reading (MA), 1975, 3: 26

附 录

附录 1 调查问卷 1

影响 IT 项目的风险因素识别与评价调查问卷

您好：

非常感谢您参与本次问卷调查活动。这是一份纯学术性问卷，旨在识别和评价影响 IT 软件项目的风险因素。

本问卷采用不记名方式，所得数据只用于科学统计分析，绝不对外公开，请您放心填答。其中的题项无所谓对错，请根据您在实际工作中的实际情况和经验，评价各风险因素的重要程度。如果某些风险因素被遗漏，请您在表格的相应空行处补充，并给出重要程度得分。若有需要，我们可将研究成果提供给贵方参考。真诚希望得到您的帮助，十分感谢！

影响 IT 软件项目的风险因素实际情况调查：1、可忽略；2、微小；3 中等；4、重要；5、十分重要，请在相应选项中打上“√”记号。下列问题各选项均为为单选题。

表 1 调查问卷 1

影响 IT 项目的风险因素			重要程度				
			1	2	3	4	5
序号	风险因素	风险描述					
1	外包决策风险	公司高层选择外包供应商决策失误					
2	供应商选择失误	对供应商的核心能力和过程能力评价不准确所造成的对供应商的选择失误					
3	需求分析不准确	对业务部门提交需求进行可行性分析不够深入，导致出现偏差					
4	需求变更风险	由于业务部门提出的需求不明确造成需求不断变更，甚至项目范围扩大					

5	设计方案出现偏差	在设计方案中，使用的实现方法不当，功能设计出现错误，功能设计考虑不周全，造成系统处理错误					
6	里程碑失控	监控计划缺陷，公司对监控环节不重视所造成的监控失控					
7	缺少用户支持	用户积极配合项目开展对项目成功至关重要，需要职能部门经理授权执行项目执行					
8	评价标准不准确	在项目合同中，对项目验收的标准，测试计划，提交的项目交付成果等等评审标准不一致					
9	软件开发达不到要求	由于技术水平，人员能力，资源条件或责任心不足所造成的结果，系统出现一些功能或影响安全运行的错误					
10	用户过高期望	项目上线后功能不能满足用户的需要，达不到用户的期望，导致期望与现实差距过大					
11	售后服务风险	技术支持人员不到位，分析问题、解决问题不及时等					
12	文档风险	文档内容描写不符合规定，描写不清楚					
13	沟通风险	发包方，供应商的协同工作机制不能发挥正常作用					
14	合同风险	由于合同签订的合同缺陷及合同类型错误选择导致出现技术和资金上的纠纷					
15	人力资源风险	人员流动特别是技术骨干力量流					

		失。					
16	进度风险	由于项目范围不断扩大或者人员安排等导致的项目延期，不能到期完成项目的问题					
17	费用风险	超过项目预期费用					
18	外包风险	主要是项目开发过程中，外包商出现问题，造成项目中断。对外包商的依赖性强，更换外包商的成本高					
19	团队管理风险	主要是制度建设、流程建设、协调控制、应急管理等方面不完善造成的团队工作问题					
20	政治法律风险	不同国家，不同主体之间由于政治体制，法律环境等差异所造成的人员，贸易，法律意识等方面的问题					
21	其他风险						
22	其他风险						
23	其他风险						
24	其他风险						
25	其他风险						

注：其他风险请您根据需要进行补充、填写。

附录 2 调查问卷 2

IT 项目风险因素之间影响关系调查问卷

您好：

首先感谢您参与本次问卷调查活动。这是一份学术性问卷，旨在研究 IT 项目中，各风险因素之间的相互影响关系。本问卷采取不记名方式，问卷调查结果仅供科研使用，请放心填写！如果您对本研究有任何意见和问题，欢迎与我们联系，共同探讨。再次对您的帮助和支持表示衷心的感谢！

表中共有 10 个风险因素，分别用 S0，S1，...，S10 表示。如果您认为表格中相应行中的风险因素对相应列中的风险因素有影响，请在对应的表格空格中打上“▲”记号。

例如，如果风险因素 S1：需求分析不准确可能影响其他所有风险因素，风险因素 S2：供应商选择失误可能影响风险因素 S5、S6、S8，风险因素 3 可能不影响其他任何风险，如下表所示。

关键风险因素		S0	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
S0	项目风险	▲										
S1	需求分析不准确	▲		▲	▲	▲	▲	▲	▲	▲	▲	▲
S2	供应商选择失误	▲					▲	▲		▲		
S3	需求变更风险	▲										

项目重要风险因素之间影响关系调查表

关键风险因素		S0	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
S0	项目风险	▲										
S1	需求分析不准确	▲										
S2	供应商选择失误	▲										
S3	需求变更风险	▲										
S4	外包决策风险	▲										
S5	缺少用户支持	▲										

S6	里程碑失控	▲										
S7	设计方案出现偏差	▲										
S8	沟通风险	▲										
S9	人力资源风险	▲										
S10	合同风险	▲										

攻读硕士学位期间取得的研究成果

序号	作者（全体作者，按顺序排列）	题 目	发表或投稿 刊物名称、级别	发表的卷 期、年月、 页码	相当于学 位论文的 哪一部分 （章、节）	被索引收 录情况

致 谢

本文是在我的导师万江平教授的亲切关怀和悉心指导下完成的。无论在课题的选题还是在课题的研究上，万老师都给了我很大的帮助。他严谨的治学作风、渊博的学识和敏锐的观察力使我受益匪浅。他不仅在学习和实践中给了我指导，在生活上给了我帮助还教会了我很多做人的道理。在此谨向万老师致以诚挚的谢意和崇高的敬意。

在此，我还要感谢在一起愉快的度过研究生生活的各位同学，正是由于你们的帮助和支持，我才能克服一个一个的困难和疑惑，直至本文的顺利完成。特别感谢我的师姐于凤娟同学，她给予我不少的帮助。

在论文即将完成之际，我的心情无法平静，从开始进入课题到论文的顺利完成，有多少可敬的师长、同学、朋友给了我无言的帮助，在这里请接受我诚挚的谢意，最后，向我的亲朋好友致谢，感谢他们对我的理解与支持，

最后，衷心的感谢我的家人在生活上和精神上对我的关怀和帮助。

再次向各方面的老师、亲人、同学和朋友们致谢！

作者：黄金和

2013 年 6 月

于华南理工大学

IV - 2 答辩委员会对论文的评定意见

论文研究了F公司软件项目风险管理研究的问题。文章通过建立ISM解释结构模型,给出了项目风险管理的五条建议,并对这五个方面分别提出软件项目关键风险规避及对策。论文书写认真规范,但是然存在一些问题,第五章需要明确关键风险规避点,不能太泛,赘述内容比较多,没有重点,应该精简,该部分需要认真修改。

在答辩中,该同学思路较为清晰、问题回答基本正确,答辩委员会一致建议授予其工商管理硕士专业学位。

论文答辩日期: 2013 年 5 月 17 日

答辩委员会委员共 3 人,到会委员 3 人

表决票数:优秀 () 票;良好 (1) 票;及格 (1) 票;不及格 (1) 票

表决结果(打“√”):优秀 ();良好 ();及格 (√);不及格 ()

决议:同意授予硕士学位 (√) 不同意授予硕士学位 ()

答辩
委员
会成
员签
名

李长 (主席)

李长

徐明