

## 第5章

# 软件项目风险管理

员工培训是企业风险最小,收益最大的战略性投资。

——沃伦·贝尼斯(Warren G. Bennis)

软件工程师总是非常乐观,当他们在计划软件项目时,经常认为每件事情都会像计划那样进行,或者会走向另外一个极端。软件开发的创造性本质,意味着软件工程师不能完全预测会发生的事情,因此制订一个详细计划的关键点很难。当有预想不到的事情引起项目脱离正常轨道时,都会导致软件项目的失败。

目前,风险管理被认为是软件项目中减少失败的一种重要手段。当不能很确定地预测将来事情的时候,可以采用结构化风险管理来发现计划中的缺陷,并且采取行动来减少潜在问题发生的可能性和影响。风险管理,意味着危机还没有发生之前就对它进行处理,这就提高了项目成功的机会,减少了不可避免风险所产生的后果。

本章共分为七部分。5.1节介绍风险概念;5.2节介绍风险管理模型;5.3节介绍风险管理计划;5.4节介绍风险识别;5.5节介绍风险分析;5.6节介绍风险监控;5.7节介绍风险管理实践。



视频讲解

## 5.1 概述

### 5.1.1 项目风险的警示

#### 1. 案例 A

瓦萨号(Vasa)是瑞典国王古斯塔夫二世于1626—1628年间下令建造的一艘军舰。1628年8月10日,瓦萨号从其建造地扬帆起航,但在航行了不到1海里后,便浸水沉没,如图5-1所示。17世纪,人们试图取回这艘沉船上颇具价值的加农炮,但在后来,这艘船便为世人所遗忘。直到1950年,有人在斯德哥尔摩港一条繁忙航线的一侧,再次找到了瓦萨号

沉船的位置。1961年4月24日,瓦萨号庞大的船躯被完整地打捞上岸,并被临时存放在瓦萨船坞(Wasavarvet)博物馆中。1987年,瓦萨号被移往斯德哥尔摩的瓦萨沉船博物馆展出。



图 5-1 博物馆陈列的瓦萨号战舰

由于在建造时没有填入足够的压舱物,瓦萨号即便在港口停靠时也不能保持平衡。尽管有着严重的结构缺陷,瓦萨号依然被允许起航。不出所料的是,在出海航行几分钟后,瓦萨号便被一阵微风吹倒,继而全船倾覆。

瓦萨号匆忙起航的因素来自以下几方面:身处国外的古斯塔夫二世急于让瓦萨号加入波罗的海舰队备战,而国王的下属们则缺少政治勇气,没有向国王禀报船只的结构缺陷,亦未请求将首航时间推延。事后,瑞典枢密院曾组织了一次针对事故的调查,以追查负责人的责任,但最后却无疾而终。

## 2. 案例 B

××信息技术有限公司(CSAI)为某省某运营商建立一个商务业务平台,并采用合作分成的方式。也就是说,所有的投资由CSAI方负担,商务业务平台投入商业应用之后运营商从所收取的收入中按照一定的比例跟CSAI分成。同一时间,平台有两个软件公司(CSAI)和G公司一起进行建设,设备以及技术均独立,也就是说,同时有两个平台提供同一种服务,两个平台分别负责不同类型的用户。

但是,整个项目进行了10个月,并经历了一个月试用期之后,准备正式投入商业应用时,运营商在没有任何通知的情况下,将该商务业务平台上所有的用户都转到了CSAI竞争对手G公司的平台上去了,也就是停止使用CSAI的商务业务平台。

## 3. 案例 C

国内一家省级电信公司(H公司)打算开发某项目,经过发布RFP需求建议书,以及谈判和评估,最终选定××信息技术有限公司(CSAI)为其提供IP电话设备。宏达公司作为CSAI的代理商,成为该项目的系统集成商。李先生是该项目的项目经理,该项目的施工周期是三个月。由CSAI负责提供主要设备,宏达公司负责全面的项目管理和系统集成工作,包括提供一些主机的附属设备和支持设备,并且负责项目的整个运作和管理。

CSAI和宏达公司之间的关系是一次性付账。这就意味着CSAI不承担任何风险,而宏

达公司虽然有很大的利润,但是也承担了全部的风险。

三个月后,整套系统安装完成。但自系统试运行之日起,不断有问题暴露出来。H公司要求宏达公司负责解决,可其中很多问题涉及CSAI的设备问题。因而,宏达公司要求CSAI予以配合。但由于开发周期的原因,CSAI无法马上达到新的技术指标并满足新的功能。于是,项目持续延期。为完成此项目,宏达公司只好不断将CSAI的最新升级系统(软件升级)提供给H公司,甚至派人常驻H公司。又经过了三个月,H公司终于通过了最初验收。在宏达公司同意承担系统升级工作直到完全满足RFP的基础上,H公司支付了10%的验收款。然而,年底,CSAI由于内部原因暂时中断了在中国的业务,其产品的支持力度大幅下降,结果致使该项目的收尾工作至今无法完成。

类似以上案例结局的项目很多,风险管理不再只是纸上谈兵,而应有具体的量化评估体系。

### 5.1.2 什么是风险管理

所谓“风险”,归纳起来主要有两种意见。主观学认为,风险是损失的不确定性;客观学认为,风险是在给定情况下一定时期可能发生的各种结果间的差异。两个基本特征是不确定性和损失。IT行业中的软件项目开发是一项可能损失的活动,不管开发过程如何进行都有可能超出预算或时间延迟。

项目风险管理实际上就是贯穿在项目开发过程中的一系列管理步骤,其中包括风险识别、风险计划、风险分析、风险解决和风险监控。它能让风险管理者主动“攻击”风险,进行有效的风险管理,如图5-2所示。

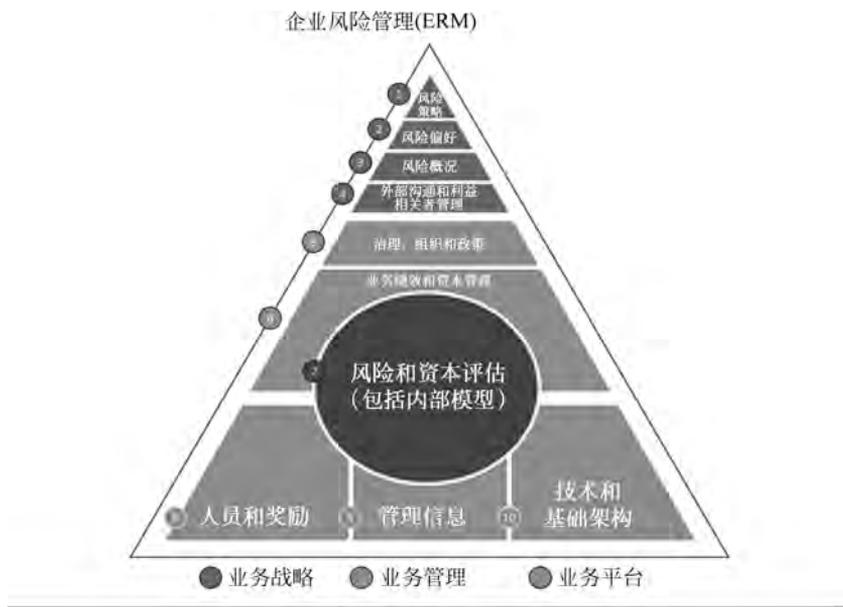


图 5-2 企业风险管理和风险控制

表 5-1 按照 3 个层次给出了风险管理规划组件。

表 5-1 风险管理规划组件

1 级	2 级	3 级
所有项目风险	业务风险	<ul style="list-style-type: none"> <li>• 竞争对手</li> <li>• 供应商</li> <li>• 现金流</li> </ul>
	技术风险	<ul style="list-style-type: none"> <li>• 硬件</li> <li>• 软件</li> <li>• 网络</li> </ul>
	组织风险	<ul style="list-style-type: none"> <li>• 执行支持</li> <li>• 用户支持</li> <li>• 团队支持</li> </ul>
	项目管理风险	<ul style="list-style-type: none"> <li>• 估计</li> <li>• 沟通</li> <li>• 资源</li> </ul>

风险管理(Risk Management)指如何在项目或者企业一个肯定有风险的环境里,把风险减至最低的管理过程。

风险管理通过对风险的认识、衡量、分析,选择最有效的方式,主动地、有目的地、有计划地处理风险,以最小成本争取获得最大安全保证的管理方法。当企业面临市场开放、法规解禁、产品创新,变化波动程度提高,连带增加经营的风险性。良好的风险管理有助于降低决策错误的概率,避免损失的可能,相对提高企业本身的附加价值。

风险管理作为企业的一种管理活动,起源于 20 世纪 50 年代的美国。当时,美国一些大公司发生了重大损失,使公司高层决策者开始认识到风险管理的重要性。其中一次,是 1953 年 8 月 12 日通用汽车公司在密歇根州的一个汽车变速器厂因火灾损失了 5000 万美元,成为美国历史上损失最为严重的 15 起重大火灾之一。这场大火与 20 世纪 50 年代其他一些偶发事件一起,推动了美国风险管理活动的兴起。

后来,随着经济、社会、技术的迅速发展,人类开始面临越来越多、越来越严重的风险。科学技术的进步在给人类带来巨大利益的同时,也给社会带来了前所未有的风险。1979 年 3 月美国三里岛核电站的爆炸事故,1984 年 12 月 3 日美国联合碳化物公司在印度的一家农药厂发生了毒气泄漏事故,1986 年切尔诺贝利核电站发生的核事故等一系列事件,大大推动了风险管理在世界范围内的发展,同时,在美国的商学院里首先出现了一门涉及如何对企业的人员、财产、责任、财务资源等进行保护的新型管理学科,就是风险管理。

目前,风险管理已经发展成企业管理中一个具有相对独立职能的管理领域,在围绕企业的经营和发展目标方面,风险管理和企业的经营管理、战略管理一样具有十分重要的意义。

风险管理能增加项目成功的概率,使项目达到预期的结果。由于软件生产的特殊性,软件风险包括软件项目风险、技术风险产品风险,如图 5-3 所示。

从项目进度、质量和成本目标看,项目管理与风险管理的目标是一致的。通过风险管理以减少风险对项目进



图 5-3 软件风险分类

度、质量、成本的影响,最终实现项目目标。从计划职能看,项目计划考虑的是未来,而未来存在不确定因素,风险管理的职能之一是减少项目整个过程中的不确定性,有利于计划的准确性。从项目实施过程看,不少风险是在项目实施过程中由潜在变成现实的,风险管理就是在风险分析的基础上拟定具体措施来消除、缓和及转移风险,并避免产生新的风险,因此有利于项目的实施。

PMP 风险管理过程包括:①风险管理计划;②风险识别;③风险定性分析;④风险定量分析;⑤风险应对计划;⑥风险监控。

CMMI 风险管理域内容如下。

特定目标 1: 风险管理标准(对应风险计划)

执行方法 1.1: 决定风险来源和类别

执行方法 1.2: 定义风险参数

执行方法 1.3: 建立风险管理策略

特定目标 2: 界定并分析风险(对应风险识别和分析)

执行方法 2.1: 界定风险

执行方法 2.2: 评估、分类及排序风险

特定目标 3: 降低风险(对应风险应对和监控)

执行方法 3.1: 开发风险降低计划

执行方法 3.2: 执行风险降低计划

风险管理的流程图如图 5-4 所示。

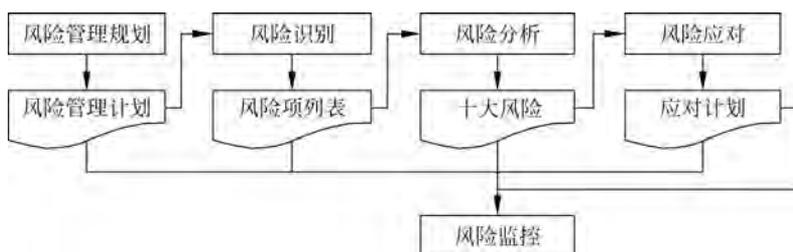


图 5-4 风险流程管理图

在 IT 软件项目管理中,应该任命一名风险管理者,该管理者的主要职责是在制订与评估规划时,从风险管理的角度对项目规划或计划进行审核并发表意见,不断寻找可能出现的任何意外情况,试着指出各个风险的管理策略及常用的管理方法,以随时处理出现的风险,风险管理者最好是由项目主管以外的人担任。



视频讲解

## 5.2 风险管理模型

针对软件项目中的风险管理问题,不少专家、组织提出了自己的风险管理模型。

### 5.2.1 玻姆模型

如图 5-5 所示,美国著名的软件工程专家、软件过程螺旋式模型之父、USC(南加州大

学)教授巴利·玻姆(Barry Boehm)用公式  $RE = P(UO) \times L(UO)$  对风险进行定义。

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、分析、设置优先级三个子步骤,风险控制则包括制订管理计划、解决和监督风险三步。

Boehm 思想的核心是十大风险因素列表,其中包括人员短缺、不合理的进度安排和预算、不断的需求变动等。针对每个风险因素,Boehm 都给出了一系列的风险管理策略。在实际操作时,以十大风险列表为依据,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十大风险因素的解决情况进行总结,产生新的十大风险因素表,以此类推。

十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。

虽然其理论存在一些不足,但 Boehm 毕竟可以说是软件项目风险管理的开山鼻祖。在其之后,更多的组织和个人开始了对风险管理的研究,软件项目风险管理的重要性日益得到认同。

### 5.2.2 持续风险管理模型

美国卡内基梅隆大学的软件工程研究所(Software Engineering Institution, SEI)作为世界上著名的旨在改善软件工程管理实践的组织,也对风险管理投入了大量的热情。SEI 提出了持续风险管理模型(Continuous Risk Management, CRM)。

SEI 的风险管理原则是:不断地评估可能造成恶劣后果的因素,决定最迫切需要处理的风险,实现控制风险的策略,评测并确保风险策略实施的有效性。

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,即风险识别、分析、计划、跟踪、控制。框架显示了应用 CRM 的基础活动及其之间的交互关系,强调了这是一个在项目开发过程中反复持续进行的活动序列。每个风险因素一般都需要按顺序经过这些活动,但是对不同风险因素开展的不同活动可以是并发的或者交替的。



图 5-5 巴利·玻姆

### 5.2.3 李维特模型

SEI 和 Boehm 的模型都以风险管理的过程为主体,研究每个步骤所需的参考信息及其操作。而丹麦奥尔堡大学(Aalborg University)提出的思路则是以李维特(Leavitt)模型为基础,着重从软件开发风险的不同角度出发探讨风险管理。

1964 年提出的李维特模型将形成各种系统的组织划分为 4 个组成部分,即任务、结构、角色、技术。

这 4 个组成部分和软件开发的各因素很好地对应起来。角色覆盖了所有的项目参与者,例如软件用户、项目经理和设计人员等;结构表示项目组织和其他制度上的安排;技术则包括开发工具、方法、硬件软件平台;任务描述了项目的目标和预期结果。李维特模型的关键思路是:模型的各个组成部分是密切相关的,一个组成部分的变化会影响其他的组成部分,如果一个组成部分的状态和其他的状态不一致,就会造成比较严重的后果,并可能降低整个系统的性能。

将这个模型和软件风险的概念相对应,即一个系统开发过程中任何李维特组成成分的修改都会产生一些问题,甚至导致软件修改的失败。根据李维特模型,任何导致风险发生的因素都可以归结为模型中的组成部分,例如技术及其可行性;或者归结为组成部分之间的联系,例如程序开发人员使用某一技术的能力。因此,使用李维特模型从四方面分别识别和分析软件项目的风险是极有条理性和比较全面的。在进行软件项目管理时,可以采用不同的方法对不同的方面进行风险管理。

李维特模型实际上是提出一个框架,可以更加广泛和系统地将软件风险的相关信息组织起来。李维特理论的设计方法和实现研究已经广泛应用于信息系统中,它所考虑的都是软件风险管理中十分重要的环节,而且简单,定义良好,适用于分析风险管理步骤。

### 5.2.4 CMMI 风险管理模型

软件能力成熟度模型集成(Capability Maturity Model Integration,CMMI)是由美国卡内基梅隆大学 SEI 在 CMM 的基础上发展而来。目前,CMMI 是全球软件业的管理标准。风险管理过程域在 CMMI 的第三级,即已定义级中建立一个关键过程域(Key Practice Area,KPA)。

CMMI 认为风险管理是一种连续的前瞻性的过程。它要识别潜在的可能危及关键目标的因素,以便策划应对风险的活动和在必要时实施这些活动,缓解不利的影响最终实现组织的目标。CMMI 的风险管理被清晰地描述为实现三个目标,每个目标的实现又通过一系列的活动来完成。

CMMI 风险管理模型如图 5-6 所示。

该模型的核心是风险库,实现各个目标的每个活动都会更新这个风险库。其中,活动“制定并维护风险管理策略”与风险库的联系是一个双向的交互过程,即通过采集风险库中相应的数据并结合前一活动的输入来制定风险管理策略。

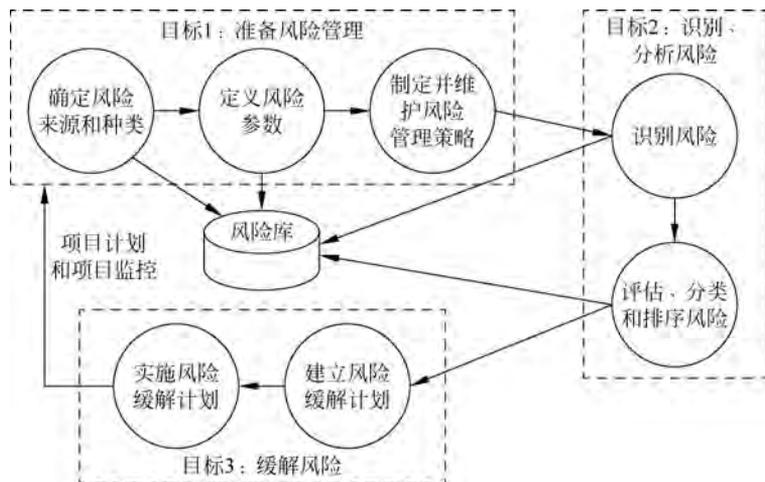


图 5-6 CMMI 风险管理模型

### 5.2.5 MSF 风险管理模型

微软解决方案框架(Microsoft Solutions Framework, MSF)的风险管理思想是,风险管理必须是主动的,它是正式和系统的过程,风险应被持续评估、监控、管理,直到被解决问题被处理。

该模型最大的特点是将学习活动融入风险管理,强调了学习以前项目经验的重要性。

它的风险管理原则是:

- (1) 持续的评估。
- (2) 培养开放的沟通环境: 所有组成员应参与风险识别与分析,领导者应鼓励建立没有责备的文化。
- (3) 从经验中学习: 学习可以大大降低不确定性,强调组织级或企业级的从项目结果中学习的重要性。
- (4) 责任分担: 组中任何成员都有义务进行风险管理。

## 5.3 风险管理计划

风险在人类的大多数活动中存在,并随时间的变化而变化,但风险是可以通过人类的活动来改变其形式和程度的,因而风险是可以管理的。

制订风险管理计划就是为了实现对风险的管理而制定一份结构完备、内容全面且互相协调的风险管理策略文件,以尽可能消除风险或尽量降低风险危害。风险管理计划对于能否成功进行项目风险管理及完成项目目标至关重要。

### 5.3.1 风险管理计划的内容

风险管理计划描述如何安排与实施项目风险管理,它是项目管理计划的从属计划。



视频讲解

## 1. 基本内容

风险管理计划的基本内容如下。

(1) 方法论。确定实施项目风险管理可使用的方法、工具及数据来源。

(2) 角色与职责。确定风险管理计划中每项活动的领导、支援与风险管理团队的成员组成。为这些角色分配人员并澄清其职责。

(3) 预算。分配资源,并估算风险管理所需费用,将之纳入项目成本基线。

(4) 计时法。确定在项目整个生命周期中实施风险管理过程的次数和频率,并确定应纳入项目进度计划的风险管理活动。

(5) 风险分类。风险分类为确保系统地、持续一致地、有效地进行风险识别提供了基础,为风险管理工作提供了一个框架。组织可使用先前准备的典型风险分类。风险分解结构(Risk Breakdown Structure,RBS)如图 5-7 所示。



图 5-7 风险分解结构图

该结构也可通过简单列明项目的各方面表述出来。在风险识别过程中需对风险类别进行重新审核,较好的做法是在风险识别过程之前,先在风险管理规划过程中对风险类别进行审查。在将先前项目的风险类别应用到现行项目之前,可能需要对原有风险类别进行调整或扩展来适应当前情况。风险分解结构列出了一个典型项目中可能发生的风险分类和风险子分类。

不同的 RBS 适用于不同类型的项目和组织,这种方法的一个好处是提醒风险识别人员风险产生的原因是多种多样的。

(6) 风险概率和影响的定义。为确保风险定性分析过程的质量和可信度,要求界定不同层次的风险概率和影响。在风险计划制订过程中,通用的风险概率水平和影响水平的界定将依据个别项目的具体情况进行调整,以便在风险定性分析过程中应用。可使用概率相对比例,例如,从“十分不可能”到“几乎确定”,或者也可分配某数值表示常规比例(例如 0.1、0.3、0.5、0.7、0.9)。测定风险概率的另外一种方法是描述与风险相关的项目状态(例如项目设计成熟度水平等)。

(7) 概率和影响矩阵。根据风险可能对实现项目目标产生的潜在影响,进行风险优先排序。风险优先排序的典型方法是借用对照表或概率和影响矩阵形式。通常由组织界定哪

些风险概率和影响组合是具有较高、中等或较低的重要性,据此可确定相应风险应对规划。在风险管理规划过程中可以进行审查并根据具体项目进行调整。

(8) 修改利害关系者承受度。可在风险管理规划过程中对利害关系者的承受水平进行修订,以适用于具体项目。

(9) 汇报格式。阐述风险登记单的内容和格式,以及所需的任何其他风险报告。界定如何对风险管理过程的成果进行记录、分析和沟通。

(10) 跟踪。说明如何记录风险活动的各方面,以便当前项目使用,或满足未来需求或满足经验教训总结过程的需要。说明是否对风险管理过程进行审计和如何审计。

## 2. 其他内容

风险管理计划的其他内容包括角色和职责、风险分析定义、低风险、中等风险和高风险的风险限界值、进行项目风险管理所需的成本和时间。

很多项目除了编制风险管理计划之外,还有应急计划和应急储备。

(1) 应急计划:是指当一项可能的风险事件实际发生时项目团队将采取的预先确定的措施。例如,当项目经理根据一个新的软件产品开发的实际进展情况,预计到该软件开发成果将不能及时集成到正在按合同进行的信息系统项目中时,他们就会启动应急计划,例如,采用对现有版本的软件产品进行少量的必要更动的措施。

(2) 应急储备:是指根据项目发起人的规定,如果项目范围或者质量发生变更,这一部分资金可以减少成本或进度风险。例如,如果由于员工对一些新技术的使用缺乏经验,而导致项目偏离轨迹,那么项目发起人可以从应急储备中拨出一部分资金,雇佣外部的顾问,为项目成员使用新技术提供培训和咨询。

### 5.3.2 制订风险管理计划的工具与技术

制订项目风险计划需要利用一些专门的技术和工具,如风险核对表技术、风险管理表格、风险数据库模式等。

#### 1. 风险核对表法

核对表是基于以前类似项目信息及其他相关信息编制的风险识别核对图表。核对表一般按照风险来源排列。利用核对表进行风险识别的主要优点是快而简单,缺点是受到项目可比性的限制。

人们考虑问题有联想习惯,在过去经验的启示下,思想常常变得很活跃,浮想联翩。风险识别实际是关于将来风险事件的设想,是一种预测。如果把人们经历过的风险事件及其来源罗列出来,写成一张核对表,那么项目管理人员看了就容易开阔思路,容易想到本项目会有哪些潜在的风险。

核对表可以包含多种内容,例如,以前项目成功或失败的原因、项目其他方面规划的结果(范围、成本、质量、进度、采购与合同、人力资源与沟通等计划成果)、项目产品或服务的说明书、项目班子成员的技能及项目可用资源等。

还可以到保险公司去索取资料,认真研究其中的保险例外,这些东西能够提醒还有哪些风险尚未考虑到。

## 2. 风险管理表格

风险管理表格记录着管理风险的基本信息。风险管理表格是一种系统地记录风险信息并跟踪到底的方式。

## 3. 风险数据库模式

风险数据库表明了识别风险和相关的信息组织方式,它将风险信息组织起来供人们查询、跟踪状态、排序和产生报告。一个简单的电子表格可作为风险数据库的一种实现,因为它能自动完成排序、报告等。风险数据库的实际内容不是计划的一部分,因为风险是动态的,并随着时间的变化而改变。

### 5.3.3 制订风险管理计划的输入输出

制订风险管理计划的输入包括:

(1) 企业环境因素:组织及参与项目的人员的风险态度和风险承受度将影响项目管理计划。风险态度和承受度可通过政策说明书或行动反映出来。

(2) 组织过程资产:组织可能设有既定的风险管理方法,例如风险分类、概念和术语的通用定义、标准模板、角色和职责、决策授权水平。

(3) 项目范围说明书。

(4) 项目管理计划。

制订风险管理计划的输出包括风险管理计划。



视频讲解

## 5.4 风险识别

### 5.4.1 风险识别概述

风险识别(Risk Identification)是企图采用系统化的方法,识别某特定项目已知的和可预测的风险。

作为用感知、判断、归类的方式对现实的和潜在的风险性质进行鉴别的过程,风险识别是风险管理的第一步,也是风险管理的基础。只有在正确识别出所面临的风险的基础上,人们才能够主动选择适当有效的方法进行处理。

存在于人们周围的风险是多样的,既有当前的,也有潜在于未来的;既有内部的,也有外部的;既有静态的,也有动态的。风险识别的任务就是要从错综复杂的环境中找出经济主题所面临的主要风险。

风险识别一方面可以通过感性认识和历史经验来判断,另一方面,也可通过对各种客观的资料和风险事故的记录来分析、归纳、整理,以及必要的专家访问,从而找出各种明显和潜在的风险及其损失规律。风险具有可变性,因而风险识别是一项持续性和系统性的工作,要求风险管理者密切注意原有风险的变化,并随时发现新的风险。

企业风险识别,指对企业面临的尚未发生的潜在的各种风险进行系统的归类分析,从而加以认识、辨别的过程。

常用方法是建立“风险条目检查表”,利用一组提问来帮助项目风险管理者了解在项目和技术方面有哪些风险。

在风险条目检查表中,列出了所有可能的与每一个风险因素有关的提问,使得风险管理者集中来识别常见的、已知的和预测的风险,如产品规模风险、依赖性风险、需求风险、管理风险及技术风险等。风险条目检查表可以以不同的方式组织,通过判定分析或假设分析,给出这些提问确定的回答,就可以帮助管理或计划人员估算风险的影响。

软件风险包含以下两个特征。

- (1) 不确定性:刻画风险的事件可能发生也可能不发生,没有100%发生的风险。
- (2) 损失:如果风险变成了现实,就会产生恶性后果或损失。

### 1. 量化损失程度

进行风险分析时,重要的是量化不确定的程度和与每个风险相关的损失的程度。为了实现这点,必须考虑以下几种不同类型的风险。

(1) 项目风险:项目风险是指潜在的预算、进度、人力(工作人员和组织)、资源、客户、需求等方面的问题以及它们对软件项目的影响。项目风险威胁项目计划,如果风险变成现实,有可能会拖延项目的进度,增加项目的成本。项目风险的因素还包括项目的复杂性、规模、结构的不确定性。

(2) 技术风险:是指潜在地设计、实现、接口、验证和维护等方面的问题。此外,规约的二义性、技术的不确定性、陈旧的技术,以及“过于先进”的技术也是风险因素。技术风险威胁要开发的软件的质量及交付时间。如果技术风险变成现实,则开发工作可能变得很困难或者不可能。

(3) 商业风险:商业风险威胁到要开发软件的生存能力。商业风险常常会危害项目或产品。

主要的商业风险包括:

- (1) 开发一个没有人真正需要的优秀产品或系统(市场风险)。
- (2) 开发的产品不再符合公司的整体商业策略(策略风险)。
- (3) 建造了一个销售部门不知道如何去卖的产品(销售风险)。
- (4) 由于重点的转移或人员的变动而失去了高级管理层的支持(管理风险)。
- (5) 没有得到预算或人力上的保证(预算风险)。

### 2. 风险方式

风险分为以下方式。

(1) 已知风险,是通过仔细评估项目计划、开发项目的商业及技术环境,以及其他可靠的信息来源(如不现实的交付时间,没有需求或软件范围的文档、恶劣的开发环境)之后可以发现的那些风险。

(2) 可预测风险,能够从过去项目的经验中推测出来(如人员调整,与客户之间无法沟通,由于需要进行维护而使开发人员精力分散)。

(3) 不可预测风险,它们可能出现,但很难事先识别出它们来。

### 3. 识别风险

识别风险是试图系统化地确定对项目计划(估算、进度、资源分配)的威胁。通过识别已

知和可预测的风险,项目管理者就有可能避免这些风险,且必要时控制这些风险。

每一类风险可以分为两种不同的类型:一般性风险和特定产品的风险。“一般性风险”,对每一个软件项目而言都是一个潜在的威胁。“特定产品的风险”,只有那些对当前项目的技术、人员及环境非常了解的人才能识别出来。为了识别特定产品的风险,必须检查项目计划及软件范围说明,从而了解本项目中有什么特殊的特性可能会威胁到项目计划。

一般性风险和特定产品的风险都应该被系统化地标识出来。识别风险的一个方法是建立风险条目检查表。该检查表可以用来识别风险,并可以集中来识别下列常见子类型中已知的及可预测的风险。

- (1) 产品规模:与要建造或要修改的软件的总体规模相关的风险。
- (2) 商业影响:与管理或市场约束相关的风险。
- (3) 客户特性:与客户的素质以及开发者和客户定期通信的能力相关的风险。
- (4) 过程定义:与软件过程被定义的程度以及它们被开发组织所遵守的程度相关的风险。
- (5) 开发环境:与用以建造产品的工具的可用性及质量相关的风险。
- (6) 建造的技术:与待开发软件的复杂性以及系统所包含技术的新奇性相关的风险。
- (7) 人员数目及经验:与参与工作的软件工程师的总体技术水平及项目经验相关的风险。

风险条目检查表能够以不同的方式来组织。与上述话题相关的问题可以由每一个软件项目来回答,这些问题的答案使得计划者能够估算风险产生的影响。

#### 1) 产品规模风险

项目风险是直接与产品规模成正比的。下面的风险检查表中的条目标识了产品(软件)规模相关的常见风险。

- (1) 是否以 LOC 或 FP 估算产品的规模?
- (2) 对于估算出的产品规模的信任程度如何?
- (3) 是否以程序、文件或事务处理的数目来估算产品规模?
- (4) 产品规模与以前产品的规模的平均值的偏差百分比是多少?
- (5) 产品创建或使用的数据库大小如何?
- (6) 产品的用户数有多少?
- (7) 产品的需求改变多少? 交付之前有多少? 交付之后有多少?
- (8) 复用的软件有多少?

#### 2) 商业影响风险

销售部门是受商业驱动的,而商业考虑有时会直接与技术实现发生冲突。下面的风险检查表中的条目标识了与商业影响相关的常见风险。

- (1) 本产品对公司的收入有何影响?
- (2) 本公司是否得到公司高级管理层的重视?
- (3) 交付期限的合理性如何?
- (4) 将会使用本产品的用户数及本产品是否与用户的需要相符合?
- (5) 本产品必须能与之互操作的其他产品/系统的数目?
- (6) 最终用户的水平如何?

- (7) 政府对本产品的开发如何约束的?
- (8) 延迟交付所造成的成本消耗是多少?
- (9) 产品缺陷所造成的成本消耗是多少?

对于待开发产品的每一个回答,都必须与过去的经验加以比较。如果出现了较大的百分比偏差或者如果数字接近过去很不令人满意的结果,则风险较高。

### 3) 客户相关风险

首先,客户有不同的需要。一些人只知道他们需要什么,而另一些人知道他们不需要什么。一些客户希望进行详细的讨论,而另一些客户则满足于模糊的承诺。

其次,客户有不同的个性。一些人喜欢享受客户的身份,而另一些人则根本不喜欢作为客户。一些人会高兴地接受几乎任何交付的产品,并能充分利用一个不好的产品,而另一些人则会对质量差的产品猛烈抨击。一些人会对质量好的产品表示赞赏,而另一些人则不管怎样都抱怨不休。

然后,客户和供应商之间也有各种不同的通信方式。一些人非常熟悉产品及生产厂商,而另一些人则可能素未谋面,仅通过信件来往和电话与生产厂商沟通。

一个“不好的”客户,可能会对一个软件项目组能否在预算内完成项目产生很大的影响。对于项目管理者而言,不好的客户是对项目计划的巨大威胁和实际的风险。下面的风险检查表中的条目,标识了与客户特征相关的常见风险。

- (1) 你以前是否曾与这个客户合作过?
- (2) 该客户是否很清楚需要什么? 他能否花时间把需求写出来?
- (3) 该客户是否同意花时间召开正式的需求收集会议,以确定项目范围?
- (4) 该客户是否愿意建立与开发者之间的快速通信渠道?
- (5) 该客户是否愿意参加复审工作?
- (6) 该客户是否具有该产品领域的技术素养?
- (7) 该客户是否愿意你的人来做他们的工作?
- (8) 该客户是否了解软件过程?

如果对于这些问题中的任何一个答案是否定的,则需要进一步的调研,以评估潜在的风险。

### 4) 过程风险

如果软件过程定义得不清楚,如果分析、设计、测试以无序的方式进行,如果质量是每个人都认为很重要的概念,但没有人切实采取行动来保证它,那么这个项目就处在风险之中。

过程问题包括:

- (1) 高级管理层是否有一份已经写好的政策陈述? 该陈述中是否强调了软件开发标准过程的重要性?
- (2) 开发组织是否已经拟定了一份已经成文的、用于本项目开发的软件过程的说明?
- (3) 开发人员是否同意按照文档所写的软件过程进行开发工作,并自愿使用它?
- (4) 该软件过程是否可以用于其他项目?
- (5) 管理者和开发人员是否接受过一系列的软件工程培训?
- (6) 是否为每一个软件开发者和管理者提供了印好的软件工程标准?
- (7) 是否为作为软件过程一部分而定义的所有交付物建立了文档概要及示例?

- (8) 是否定期对需求规约、设计和编码进行正式的技术复审?
- (9) 是否定期对测试过程和测试情况进行复审?
- (10) 是否对每一次正式技术复审的结果建立了文档,其中包括发现的错误及使用的资源?
- (11) 是否有什么机制能保证按照软件工程标准来指导工作?
- (12) 是否使用配置管理来维护系统/软件需求、设计、编码、测试用例之间的一致性?
- (13) 是否使用一个机制来控制用户需求的变化及其对软件的影响?
- (14) 对于每一个承包出去的子合同,是否有一份文档化的工作说明、一份软件需求规约和一份软件开发计划?
- (15) 是否有一个可遵循的规程来跟踪及复审子合同承包商的工作?

技术问题包括:

- (1) 是否使用方便易用的规格说明技术来辅助客户与开发者之间的通信?
- (2) 是否使用特定的方法进行软件分析?
- (3) 是否使用特定的方法进行数据和体系结构的设计?
- (4) 是否 90% 以上的代码都是使用高级语言编写的?
- (5) 是否定义及使用特定的规则进行代码编写?
- (6) 是否使用特定的方法进行测试用例的设计?
- (7) 是否使用配置管理软件工具控制和跟踪软件过程中的变化活动?
- (8) 是否使用工具来创造软件原型?
- (9) 是否使用软件工具来支持测试过程?
- (10) 是否使用软件工具来支持文档的生成和管理?
- (11) 是否收集所有软件项目的质量度量值?
- (12) 是否收集所有软件项目的生产率度量值?

如果对于上述问题的答案多数是否定的,则软件过程是薄弱的,且风险很高。

#### 5) 技术风险

突破技术的极限极具挑战性和令人兴奋,但这也是有风险的。下面的风险检查表中的条目标识了与建造的技术相关的常见风险。

- (1) 该技术对于你的公司而言是新的吗?
- (2) 客户的需求是否需要创建新的算法或输入、输出技术?
- (3) 待开发的软件是否需要使用新的或未经证实的硬件接口?
- (4) 待开发的软件是否需要与开发商提供的未经证实的软件产品接口?
- (5) 待开发的软件是否需要与功能和性能均未在本领域得到证实的数据库系统接口?
- (6) 产品的需求是否要求采用特定的用户界面?
- (7) 产品的需求中是否要求开发某些程序构件,这些构件与你的公司以前开发的构件是否完全不同?
- (8) 需求中是否要求采用新的分析、设计、测试方法?
- (9) 需求中是否要求使用非传统的软件开发方法?
- (10) 需求中是否有过分的对产品的性能约束?
- (11) 客户能确定所要求的功能是可行的吗?

如果对于这些问题中的任何一个答案是肯定的,则需要进一步的调研,以评估潜在的风险。

#### 6) 开发环境风险

软件工程环境支持项目组、过程及产品,但是,如果环境有缺陷,它就有可能成为重要的风险源。下面的风险检查表中的条目,标识了与开发环境相关的风险。

- (1) 是否有可用的软件项目管理工具?
- (2) 是否有可用的软件过程管理工具?
- (3) 是否有可用的分析及设计工具?
- (4) 分析和设计工具是否适用于待建造产品?
- (5) 是否有可用的编译器或代码生成器?
- (6) 是否有可用的测试工具?
- (7) 是否有可用的软件配置管理工具?
- (8) 环境是否利用了数据库或数据仓库?
- (9) 项目组的成员是否接受过每个所使用工具的培训?
- (10) 是否有专家能够回答有关工具的问题?
- (11) 工具的联机帮助及文档是否适当?

如果对于上述问题的答案多数是否定的,则软件开发环境是薄弱的,且风险很高。

#### 7) 与人员数目及经验相关的风险

与人员数目及经验相关的风险包括:

- (1) 是否有最优秀的人员可用?
- (2) 人员在技术上是否配套?
- (3) 是否有足够的人员可用?
- (4) 开发人员是否能够自始至终地参加整个项目的工作?
- (5) 项目中是否有一些人员只能部分时间工作?
- (6) 开发人员对自己的工作是否有正确的期望?
- (7) 开发人员是否接受过必要的培训?
- (8) 开发人员的流动是否仍能保证工作的连续性?

如果对于这些问题中的任何一个答案是否定的,则需要进一步的调研,以评估潜在的风险。

## 5.4.2 用于风险识别的方法

### 1. 分析识别的步骤

风险识别一般可分为以下三步进行。

(1) 收集资料。资料和数据能否到手、是否完整必然会影响项目风险损失的大小。能帮助我们识别风险的资料包括项目产品或服务的说明书;项目的前提、假设和制约因素;与本项目类似的案例。

(2) 风险形势估计。风险形势估计是要明确项目的目标、战略、战术、实现项目目标的手段和资源以及项目的前提和假设,以正确确定项目及其环境的变数。

(3) 根据直接或间接的症状将潜在的风险识别出来。

风险识别首先需要对制订的项目计划、项目假设条件和约束因素、与本项目具有可比性的已有项目的文档及其他信息进行综合会审。风险的识别可以从原因查结果,也可以从结果反过来找原因。

## 2. 风险识别的具体方法

在具体识别风险时,需要综合利用一些专门技术和工具,以保证高效率地识别风险并不发生遗漏,这些方法包括德尔菲法、头脑风暴法、检查表法、SWOT 技术、检查表和图解技术等。现将方法简要介绍如下。

### 1) 德尔菲技术

如 3.3.1 节所述,德尔菲技术是众多专家就某一专题达成一致意见的一种方法。项目风险管理专家以匿名方式参与此项活动。主持人用问卷征询有关重要项目风险的见解,问卷的答案交回并汇总后,随即在专家之中传阅,请他们进一步发表意见。此项过程进行若干轮之后,就不难得出关于主要项目风险的一致看法。德尔菲技术有助于减少数据中的偏倚,并防止任何个人对结果不适当地产生过大的影响。

### 2) 头脑风暴法

如 2.3.3 节所述,头脑风暴法的目的是取得一份综合的风险清单。头脑风暴法通常由项目团队主持,虽然也可邀请多学科专家来实施此项技术。在一位主持人的推动下,与会人员就项目的风险进行集思广益。可以以风险类别作为基础框架,然后再对风险进行分门别类,并进一步对其定义加以明确。

### 3) SWOT 分析法

SWOT 分析法是一种环境分析方法。所谓的 SWOT 是英文 Strength(优势)、Weakness(劣势)、Opportunity(机遇)和 Threat(挑战)的简写,如图 5-8 所示。



图 5-8 SWOT 分析法

SWOT 分析是列出项目的优势和劣势、可能的机会与威胁,填入道斯矩阵的 I、II、III、IV 区。道斯矩阵如图 5-9 所示。

	III 优势 列出自身的优势	IV 劣势 具体列出弱点
I 机会 列出现有的机会	V SO 战略 抓住机遇,发挥优势战略	VI WO 战略 利用机会,克服劣势战略
II 挑战 列出正面临的威胁	VII ST 战略 利用优势,减少威胁战略	VIII WT 战略 弥补缺点,规避威胁战略

图 5-9 道斯矩阵

SWOT 分析一般分为如下 5 步。

(1) 将内部优势与外部机会相组合,形成 SO 策略,制定抓住机遇、发挥优势的战略,填

入道斯矩阵的V区。

(2) 将内部劣势与外部机会相组合,形成WO策略,制定利用机遇、克服劣势的战略,填入道斯矩阵的VI区。

(3) 将内部优势与外部威胁相组合,形成ST策略,制定利用优势、减少威胁战略,填入道斯矩阵的VII区。

(4) 将内部劣势与外部挑战相组合,形成WT策略,制定弥补缺点、规避威胁的战略,填入道斯矩阵的VIII区。

#### 4) 检查表

检查表(Check List)是管理中用来记录和整理数据的常用工具,如表5-3所示。

在进行风险识别时,将项目可能发生的许多潜在风险列于一个表上,供识别人员进行检查核对,用来判别某项目是否存在表中所列或类似的风险。

检查表中所列都是历史上类似项目曾发生过的风险,是项目风险管理经验的结晶,对项目管理人员具有开阔思路、启发联想、抛砖引玉的作用。一个成熟的项目公司或项目组织,要掌握丰富的风险识别检查表工具,如表5-2所示。

表 5-2 项目演变过程中可能出现的风险因素检查表

生命周期	可能的风险因素
全过程	<ul style="list-style-type: none"> <li>✧ 对一个或更多阶段的投入时间不够</li> <li>✧ 没有记录下重要的信息</li> <li>✧ 尚未结束一个或更多前期阶段就进入下一阶段</li> </ul>
概念	<ul style="list-style-type: none"> <li>✧ 没有书面记录下所有的背景信息与计划</li> <li>✧ 没有进行正式的成本-收益分析</li> <li>✧ 没有进行正式的可行性研究</li> <li>✧ 不知道是谁首先提出项目创意</li> </ul>
计划	<ul style="list-style-type: none"> <li>✧ 准备计划的人过去没有承担过类似的项目</li> <li>✧ 没有写下项目计划的某些部分</li> <li>✧ 遗漏了项目计划的某些部分</li> <li>✧ 项目计划的部分或全部没有得到所有关键成员的批准</li> <li>✧ 指定完成项目的人不是准备计划的人</li> <li>✧ 未参加制订项目计划的人没有审查项目计划,也未提出任何疑问</li> </ul>
执行	<ul style="list-style-type: none"> <li>✧ 主要客户需求发生变化</li> <li>✧ 收集到的有关进度情况和资源消耗的信息不够完整或不够准确</li> <li>✧ 项目进展报告不一致</li> <li>✧ 一个或更多找到的项目支持者有了新的分配任务,项目成员就被分配到新的项目组中</li> <li>✧ 在实施期间替换了项目组的成员</li> <li>✧ 市场特征或需求发生了变化</li> <li>✧ 做了非正式的变更,并且没有对它们带给整个项目的影响做出分析</li> </ul>
结束	<ul style="list-style-type: none"> <li>✧ 一个或更多的项目驱使着没有正式批准项目的成果</li> <li>✧ 在尚未完成项目的所有工作下,项目成员被分配到新的项目组</li> </ul>

#### 5) 图解技术

图解技术包括如下内容。

(1) 因果图(Cause-and-Effect Diagram): 又被称作石川图或鱼骨图,用于识别风险的

成因,如图 5-10 所示。



图 5-10 因果图

(2) 系统或过程流程图(Flow Chart): 显示系统的各要素之间如何相互联系以及因果传导机制。

(3) 影响图(Influence Diagram): 显示因果影响。影响图是不确定条件下决策制定的图形辅助工具,将一个项目或项目中的一种情境表现为一系列实体、结果、影响,以及之间的关系和相互影响。如果因为存在单个项目风险或其他不确定性来源,使影响图中的某些要素不确定,就在影响图中以区间或概率分布的形式表示这些要素。然后,借助模拟技术(如蒙特卡罗分析, Monte Carlo Analysis)来分析哪些要素对重要结果具有最大的影响,如图 5-11 所示。

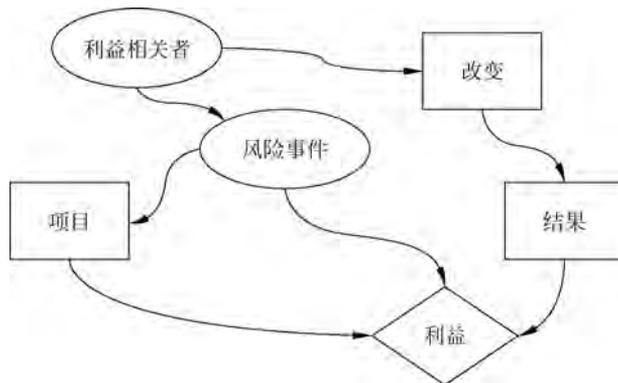


图 5-11 影响图

### 5.4.3 风险识别的输入输出

#### 1. 风险识别的输入

风险识别的输入包括如下几方面。

(1) 企业环境因素: 在风险识别过程中,可依据公布的信息,例如商业数据库、学术研究、基准参照或其他行业研究作用。

(2) 组织过程资产: 可从先前项目的项目档案中获得相关信息,包括实际数据和经验

教训。

(3) 项目范围说明书：通过项目范围说明书可查到项目假设条件信息。有关项目假设条件的不确定性,应作为项目的潜在风险,进行评估。

(4) 风险管理计划：风险管理计划向风险识别过程提供的主要依据信息包括角色和职责的分配、预算和进度计划中纳入的风险管理活动因素、风险类别。风险类别有时可用风险分解结构形式表示。

(5) 项目管理计划：风险识别过程也要求对项目管理计划中的进度、成本和质量管理计划有所了解。应对其他知识领域过程的成果进行审查,以确定跨越整个项目的可能风险。

## 2. 风险识别的输出

风险识别的输出是风险登记表。风险识别过程的主要成果形成项目管理计划中风险登记表的最初记录。最终,风险登记表也将包括其他风险管理过程的成果。风险登记表的编制始于风险识别过程,其中记录的信息也可供其他项目管理过程和项目风险管理过程使用。所记录的主要信息如下。

(1) 已识别风险清单：在此对已识别风险进行描述,包括其根本原因、不确定的项目假设等。

(2) 潜在应对措施清单：在风险识别过程中,可识别风险的潜在应对措施。如此确定的风险应对措施可作为风险应对规划过程的依据。

(3) 风险基本原因：指可导致已识别风险的基本状态或事件。

(4) 风险类别更新：在识别风险的过程中,可能会识别新的风险类别,进而将新风险类别纳入风险类别清单中。基于风险识别过程的成果,可对风险管理规划过程中形成的风险分解结构进行修改或完善。

## 5.5 风险分析

风险分析(Risk Analysis)有狭义和广义两种。

狭义的风险分析指通过定量分析的方法给出完成任务所需的费用、进度、性能三个随机变量的可实现值的概率分布。广义的风险分析则是一种识别和测算风险,开发、选择、管理方案来解决这些风险的有组织的手段,包括风险识别、风险评估、风险管理三方面的内容。

风险识别确定哪些可能导致费用超支、进度推迟、性能降低的潜在问题,并定性分析其后果。在这一步须做的工作,是分析系统的技术薄弱环节及不确定性较大之处,得出系统的风险源,并将这些风险源组合成一格式文件,供以后分析参考。风险分析对潜在问题可能导致的风险及其后果实行量化,并确定其严重程度。

其中,可能牵涉到多种模型的综合应用,最后得到系统风险的综合印象。风险管理在风险识别及风险分析的基础上,采取各种措施来减小风险及对风险实施监控。这也可以说是风险分析的最终目的。

风险分析对风险影响和后果进行评价和估量,包括定性分析和定量分析。①定性分析是评估已识别风险的影响和可能性的过程,按风险对项目目标可能的影响进行排序。作用和目的为识别具体风险和指导风险应对,根据风险对项目目标的潜在影响对风险进行排序,通过比较风险值确定项目总体风险级别。②定量分析是量化分析每一风险的概率及其对项目目标造成的后果,也分析项目总体风险的程度。作用和目的为测定实现某一特定项目目



视频讲解

标的概率,通过量化各个风险对项目目标的影响程度,甄别出最需要关注的风险,识别现实的和实现的成本、进度、范围目标。

### 5.5.1 定性风险分析

定性风险分析指通过考虑风险发生的概率、风险发生后对项目目标及其他因素(即费用进度范围和质量风险承受度水平)的影响,对已识别风险的优先级进行评估。

通过概率和影响级别定义,以及专家访谈可有助于纠正该过程所使用的数据中的偏差,相关风险行动的时间紧迫性可能会夸大风险的严重程度。对目前已掌握的项目风险信息的质量进行评估有助于理解有关风险对项目重要性的评估结果。

#### 1. 定性风险分析的方法

定性风险分析的方法有风险概率与影响评估、概率和影响矩阵、风险分类、风险紧迫性评估等。

##### 1) 风险概率与影响评估

风险概率指调查每项具体风险发生的可能性,风险影响评估旨在分析风险对项目目标(如时间、费用、范围或质量)的潜在影响,既包括消极影响或威胁,也包括积极影响或机会。

可通过挑选对风险类别熟悉的人员采用召开会议或进行访谈等方式对风险进行评估,其中包括项目团队成员和项目外部的专业人士。组织的历史数据库中关于风险方面的信息可能寥寥无几,此时需要专家做出判断,由于参与者可能不具有风险评估方面的任何经验,因此需要由经验丰富的主持人引导讨论。

在访谈或会议期间对每项风险的概率级别及其对每项目标的影响进行评估,其中也需要记载相关的说明信息,包括确定概率和影响级别所依赖的假设条件等,根据风险管理计划中给定的定义,确定风险概率和影响的等级。有时风险概率和影响明显很低,此种情况下,不会对之进行等级排序,而是作为待观察项目列入清单中供将来进一步监测。

##### 2) 概率和影响矩阵

根据评定的风险概率和影响级别,对风险进行等级评定。通常采用参照表的形式或概率影响矩阵的形式,评估每项风险的重要性及其紧迫程度。概率和影响矩阵形式规定了各种风险概率和影响组合,并规定哪些组合被评定为高重要性、中重要性或低重要性。

对目标的影响,每一风险按其发生概率及一旦发生所造成的影响评定级别。矩阵中所示组织规定的低风险、中等风险与高风险的临界值确定了风险的得分。

组织应确定哪种风险概率和影响的组合可被评定为高风险(红灯状态)、中等风险(黄灯状态)或低风险(绿灯状态)。在黑白两种色彩组成的矩阵中,这些不同的状态可分别用不同深度的灰色代表,深灰色(数值最大的区域)代表高风险,中度灰色区域(数值最小)代表低风险,而浅灰色区域(数值介于最大和最小值之间)代表中等程度风险。通常,由组织在项目开展之前提前界定风险等级评定程序。

风险分值可为风险应对措施提供指导。例如,如果风险发生会对项目目标产生不利影响(即威胁),并且处于矩阵高风险(深灰色)区域,可能就需要采取重点措施,并采取积极的应对策略。而对于处于低风险区域(中度灰色)的威胁,只需将之放入待观察风险清单或分配应急储备,无须额外采取任何其他直接管理措施。

同样,对于处于高风险(深灰色)区域的机会,最容易实现而且能够带来最大的利益,所以应先以此为工作重点。对于低风险(中度灰色)区域的机会应对之进行监测。

### 3) 风险分类

可按照风险来源(使用风险分解矩阵)、受影响的项目区域(使用工作分解结构)或其他分类标准(例如项目阶段)对项目风险进行分类,以确定受不确定性影响最大的项目区域。根据共同的根本原因对风险进行分类,有助于制定有效的风险应对措施。

### 4) 风险紧迫性评估

需要近期采取应对措施的风险可被视为亟须解决的风险。实施风险应对措施所需的时间、风险征兆、警告和风险等级都可作为确定风险优先级或紧迫性的指标。

## 2. 定性风险分析的输入输出

### 1) 定性风险分析的输入

(1) 组织过程资产:在进行风险定性分析过程中,可借用先前项目的风险数据及经验教训知识库。

(2) 项目范围说明书:常见或反复性的项目对风险事件发生概率及其后果往往理解比较透彻。而采用新技术或创新性技术的项目或者极其复杂的项目,其不确定性往往要大许多。可通过检查项目范围说明书对此进行评估。

(3) 风险管理计划:风险管理计划中用于风险定性分析的关键元素包括风险管理角色和职责、风险管理预算和进度活动、风险类别、概率和影响的定义以及概率和影响矩阵及相关干系人承受度。在风险管理规划过程中,通常按照项目具体情况对这些元素进行调整。如果这些元素不存在,可在风险定性分析过程中建立这些元素。

(4) 风险登记单:就风险定性分析而言,来自风险登记单的一项关键依据是已识别风险的清单。

### 2) 定性风险分析的输出

定性风险分析的输出是风险登记单。风险登记单是在风险识别过程中形成的,并根据风险定性分析的信息进行更新,将更新后的风险登记单纳入项目管理计划之中。依据风险定性分析对风险登记单进行更新的内容如下。

(1) 项目风险的相对排序或优先度清单:可使用风险概率和影响矩阵,根据风险的重要程度进行分类。项目经理可参考风险优先度清单,集中精力处理高重要性的风险,以获得更好的项目成果。如果组织更关注其中一项目标,则可分别为成本、进度、范围和质量目标单独列出风险优先度。对于被评定为对项目十分重要的风险而言,应对其风险概率和影响的评定基础和依据进行描述。

(2) 按照类别分类的风险:进行风险分类,可揭示风险的共同原因或特别需要关注的项目领域。在发现风险集中的领域之后,可提高风险应对的有效性。

(3) 需要在近期采取应对措施的风险清单:需要采取紧急应对措施的风险和可在今后某些时候处理的风险应分入不同的类别。

(4) 需要进一步分析与应对的风险清单:有些风险可能需要进一步分析,包括风险定量分析以及采取风险应对措施。

(5) 低优先度风险观察清单:在风险定性分析过程中把评为不重要的风险放入观察清单中,进行进一步监测。

(6) 风险定性分析结果的趋势: 在分析重复进行后, 特定风险的分析结果可能出现某种明显趋势, 从而采取应对措施或者进一步进行分析变得比较紧迫或者比较重要。

## 5.5.2 定量风险分析

定量风险分析是指对定性风险分析过程中识别出的对项目需求存在潜在重大影响而排序在前的风险进行的量化分析, 并就风险分配一个数值。风险定量分析是在不确定情况下进行决策的一种量化的方法。该项目过程采用蒙特卡罗模拟与决策树分析等技术。

- (1) 对项目结果以及实现项目结果的概率进行量化。
- (2) 评估实现具体项目目标的概率。
- (3) 通过量化各项风险对项目总体风险的影响确定需特别重视的风险。
- (4) 在考虑项目风险的情况下确定可以实现的切合实际的成本进度或范围目标。
- (5) 在某些条件或结果不确定时确定最佳的项目管理决策。

下面来看看数据收集和表示的方法及应用。

### 1. 期望货币值

期望货币值(Expected Monetary Value, EMV)是一个统计概念, 用以计算在将来某种情况发生或不发生情况下的平均结算(即不确定状态下的分析)。

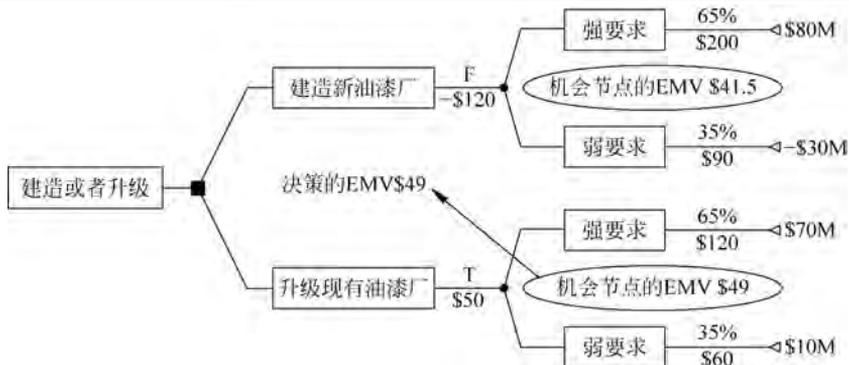
预期货币值和决策树一起使用, 是将特定情况下可能的风险造成的货币后果和发生概率相乘, 项目包含风险和现金的考虑。正值表示机会, 负值表示风险。

机会的期望货币价值一般表示为正数, 而风险的期望货币价值一般被表示为负数。每个列结果的数值与其发生概率相乘之后加总, 即得出期望货币价值。这种分析最通常的用途是用于决策树分析。

决策树是对所考虑的决策以及采用现有方案可能产生的后果进行描述的一种图解方法, 如表 5-3 所示。它综合了每项可用选项的成本和概率以及每条事件逻辑路径的收益。当所有收益和后续决策全部量化之后, 决策树的求解过程可得出每项方案的预期货币价值或组织关心的其他衡量指标。

表 5-3 决策树分析

决策定义	决策节点	机会节点	纯路径价值
制定决策	依据: 每项选择成本 成果: 已定决策(对、错)	依据: 情景概率发生后的奖励 成果: 期望现金价值	计算 (盈利减去成本)沿路径



## 2. 计算分析因子

人们通常按照高、中、低来描述风险概率。为了量化风险的概率和后果,美国国防系统管理学院开发了一项技术,用于计算风险因子——求各种具体事件的整体风险的数字(基于其发生的概率和对项目造成的结果)。这项技术使用概率和影响矩阵显示风险发生的概率或可能性,以及风险的影响或结果。

## 3. 计划评审技术

计划评审技术(Program/Project Evaluation and Review Technique, PERT)是利用网络分析制订计划以及对计划予以评价的技术,能协调整个计划的各道工序,合理安排人力、物力、时间和资金加速计划的完成。

PERT网络是一种类似流程图的箭线图,描绘出项目包含的各种活动的先后次序,标明每项活动的时间或相关的成本。

对于PERT网络,项目管理者必须考虑要撤掉哪些工作,确定时间之间的依赖关系辨认出潜在的可能出问题的环节,借助PERT还可以方便地比较不同行动方案在进度和成本方面的效果。

PERT首先是建立在网络计划基础之上的,其次是工程项目中各个工序的工作时间不肯定,过去通常对这种计划只是估计一个时间,到底完成任务的把握有多大,决策者心中无数,工作处于一种被动状态。在工程实践中,由于人们对事物的认识受到客观条件的制约,通常在PERT中引入概率计算方法,由于组成网络计划的各项工作可变因素多,不具备一定的时间消耗统计资料,因而不能确定出一个肯定的单一的时间值。

在PERT中,假设各项工作的持续时间服从 $p$ 分布,近似地用三时估计法估算出三个时间值,即最短、最长和最可能持续时间,再加权平均算出一个期望值作为工作的持续时间。在编制PERT网络计划时,把风险因素引入到PERT中,人们不得不考虑按PERT网络计划在指定的工期下完成工程任务的可能性有多大,即计划的成功概率,也就是计划的可靠度,这就必须对工程计划进行风险估计。

在绘制网络图时必须将非肯定型转换为肯定型,把三时估计变为单一时间估计,其计算公式为:

$$T = \frac{T_o + 4T_m + T_p}{6}$$

其中:

$T$ : 被估算工作的平均持续时间。

$T_o$ : 被估算工作最短持续时间(乐观估计时间)。

$T_p$ : 被估算工作最长持续时间(悲观估计时间)。

$T_m$ : 被估算工作正常持续时间,可由施工定额估算。

## 4. 蒙特卡罗分析

蒙特卡罗(Monte Carlo)方法又称为统计模拟法、随机抽样技术,是一种随机模拟方法,以概率和统计理论方法为基础,是使用随机数(伪随机数)来解决很多计算问题的方法。将所求解的问题同一定的概率模型相联系,用计算机实现统计模拟或抽样,以获得问题的近似解。

蒙特卡罗方法由美国在第二次世界大战中研制原子弹的“曼哈顿计划”计划的成员斯塔尼斯拉夫·乌拉姆(Stanisław Marcin Ulam)和冯·诺依曼(von Neumann)于20世纪40年代提出。冯·诺依曼用驰名世界的赌城摩纳哥的蒙特卡罗来命名这种方法,为它蒙上了一层神秘色彩。1777年,法国布丰(Buffon)提出用投针实验的方法求圆周率 $\pi$ ,这被认为是蒙特卡罗方法的起源,如图5-12所示。

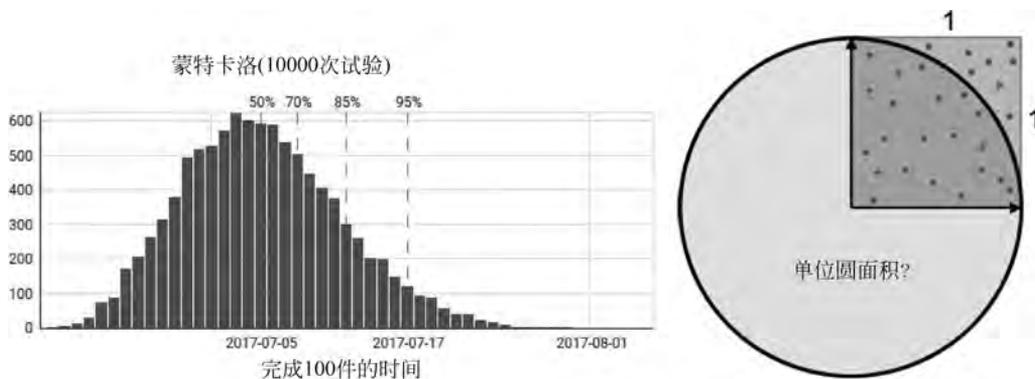


图 5-12 蒙特卡罗分析

蒙特卡罗的基本步骤如下。

(1) 针对现实问题建立一个简单且便于实现的概率统计模型,使所求的解恰好是所建立模型的概率分布或其某个数字特征,例如某个事件的概率或者该模型的期望值。

(2) 对模型中的随机变量建立抽样方法,在计算机上进行模拟实验,抽取足够的随机数,并对相关的事件进行统计。

(3) 对模拟结果加以分析,给出所求解的估计及其方差的估计。必要时改进模型以提高估计精度和模拟计算的效率。在这种模拟中,项目模型经过多次计算(叠加),其随机依据值来自根据每项变量的概率分布,为每个迭代过程选择概率分布函数(例如项目元素的费用或进度活动的持续时间),据此计算概率分布(例如总费用或完成日期)。对于成本风险分析,可用传统的项目工作分解结构或成本分解结构作为模拟。对于进度风险分析,可用优先顺序图法(Precedence Diagramming Method,PDM)。

### 5.5.3 定量风险分析的输入输出

#### 1. 定量风险分析的输入

定量风险分析的输入有如下项目。

(1) 组织过程资产:包括先前完成的类似项目的信息、风险专家对类似项目的研究以及行业或专有渠道获得的风险数据库。

(2) 项目范围说明书。

(3) 风险管理计划:就风险定量分析而言,风险管理计划的关键要素包括风险管理角色和职责、风险管理预算和进度活动、风险类别、风险分解结构和修改的利害关系者风险承受度。

(4) 风险登记表：就风险定量分析而言，风险登记表的项目包括已识别风险列表、项目风险的相对排序或优先度表以及按照类别归类的风险。

(5) 项目管理计划：包括项目进度管理计划和项目费用管理计划。项目进度管理计划为项目进度的制定和控制规定了格式和标准。项目费用管理计划为项目费用的规划、架构、估算、预算和控制规定了格式和标准。

## 2. 定量风险分析的输出

定量风险分析的输出是风险登记表(更新)。风险登记表在风险识别过程中形成，并在风险定性分析过程中更新。在风险定量分析过程中会进一步更新。风险登记表是项目管理计划的组成部分。此处的更新内容如下。

(1) 项目的概率分析：项目潜在进度与成本结果的预报，并列出的可能的竣工日期或项目工期与成本及其可信度水平。该项成果(通常以累积分布表示)与利害关系者的风险承受度水平结合在一起，以对成本和时间应急储备金进行量化。需要把应急储备金将超出既定项目目标的风险降低到组织可接受的水平。

(2) 实现成本和时间目标的概率：采用目前的计划以及目前对项目所面临的风险的了解，可用风险定量分析方法估算出实现项目目标的概率。

## 5.5.4 应对风险的基本措施

通过对项目风险识别、估计和评价，把项目风险发生的概率、损失严重程度以及其他因素综合起来考虑，可得出项目发生各种风险的可能性及其危害程度，再与公认的安全指标相比较，就可确定项目的危险等级，从而决定应采取什么措施以及控制措施应采取到什么程度。风险应对就是对项目风险提出处置意见和办法。项目风险的应对包括对风险有利机会的跟踪和对风险不利影响的控制。

因此，风险应对规划策略可分为以下三种。

### 1. 消极风险或威胁的应对策略

通常使用三种策略应对可能对项目目标存在消极影响的风险或威胁。这些策略分别是规避、转移与减轻。

#### 1) 规避

规避风险是指改变项目计划，以排除风险或条件，或者保护项目目标，使其不受影响，或对受到威胁的一些目标放松要求，例如延长进度或减少范围等。但是这是相对保守的风险对策，在回避风险的同时也就彻底放弃了项目带给我们的各种收益和发展机会。

规避风险的另一个重要的策略是排除风险的起源，即利用分隔将风险源隔离于项目进行的路径之外。事先评估或筛选适合于本身能力的风险环境进入经营，包括细分市场的选择、供货商的筛选等，或选择放弃某项环境领域，以准确预见并有效防范，完全消除风险的威胁。

我们经常听到的项目风险管理 80-20 规律(参见第 1 章)告诉我们，项目所有风险中对项目产生 80%威胁的只是其中的 20%的风险，因此要集中力量去规避 20%的最危险的风险。

## 2) 转移

转移风险是指设法将风险的后果连同应对的责任转移到他方身上,转移风险实际只是把风险损失的部分或全部以正当理由让他方承担,而非将其拔除。

风险转移策略几乎总需要向风险承担者支付风险费用。转移工具丰富多样,包括但不限于利用保险、履约保证书、担保书和保证书。出售或外包将自己不擅长的或自己开展风险较大的一部分业务委托他人帮助开展,集中力量在自己的核心业务上,从而有效地转移风险。同时,可以利用合同将具体风险的责任转移给另一方。

在多数情况下,使用费用加合同可将费用风险转移给买方,如果项目的设计是稳定的,可以用固定总价合同把风险转移给卖方。有条件的企业可运用一些量化的风险决策分析方法和工具来精算优化保险方案。

## 3) 减轻

减轻是指设法把不利的风险事件的概率或后果降低到一个可接受的临界值。提前采取行动减少风险发生的概率或者减少其对项目所造成的影响,比在风险发生后亡羊补牢进行的补救要有效得多。例如,设计时在系统中设置冗余组件有可能减轻原有组件故障所造成的影响。

## 2. 接受

采取该策略的原因在于很少可以消除项目的所有风险。

采取此项措施表明,已经决定不打算为处置某项风险而改变项目计划,无法找到任何其他应对良策的情况下,或者为应对风险而采取的对策所需要付出的代价太高(尤其是当该风险发生的概率很小时),往往采用“接受”这一措施。针对机会或威胁,均可采取该项策略。

该策略可分为主动或被动方式。最常见的主动接受风险的方式就是建立应急储备,应对已知或潜在的未知威胁或机会。被动地接受风险则不要求采取任何行动,将其留给项目团队,待风险发生时视情况进行处理。

## 3. 积极风险或机会的应对策略

通常,使用三种策略应对可能对项目目标存在积极影响的风险。这些策略分别是开拓、分享和提高。

(1) 开拓:如果组织希望确保机会得以实现,可就具有积极影响的风险采取该策略。该项策略的目的在于通过确保机会肯定实现而消除与特定积极风险相关的不确定性。直接开拓措施,包括为项目分配更多的有能力的资源,以便缩短完成时间或实现超过最初预期的高质量。

(2) 分享:分享积极风险是指将风险的责任分配给能为项目的利益获取机会的第三方,包括建立风险分享合作关系,或专门为机会管理目的形成团队、特殊目的项目公司或合作合资企业。

(3) 提高:该策略旨在通过提高积极风险的概率或其积极影响,识别并最大程度发挥这些积极风险的驱动因素,致力于改变机会的“大小”。通过促进或增强机会的成因,积极强化其触发条件,提高机会发生的概率,也可着重针对影响驱动因素以提高项目机会。

## 5.6 风险监控

风险监控(Risk Monitoring and Control)在决策主体的运行过程中,对风险的发展与变化情况进行全程监督,并根据需要进行应对策略的调整。因为风险是随着内部外部环境的变化而变化的,在决策主体经营活动的推进过程中,可能会增大或者衰退乃至消失,也可能由于环境的变化又生成新的风险。

项目风险监控是通过对风险规划、识别、估计、评价、应对全过程的监视和控制,从而保证风险管理能达到预期的目标,是项目实施过程中的一项重要工作。

监控风险实际是监视项目的进展和项目环境,即项目情况的变化,目的是核对风险管理策略和措施的实际效果是否与预见的相同,寻找机会改善和细化风险规避计划,获取反馈信息,以便将来的决策更符合实际。风险监控过程中,及时发现那些新出现的以及随着时间推延而发生变化的风险,然后及时反馈,并根据对项目的影响程度,重新进行风险规划、识别、估计、评价、应对。

风险监控就是要跟踪风险,识别剩余风险和新出现的风险,修改风险管理计划,保证风险计划的实施,并评估消减风险的效果,从而保证风险管理能达到预期的目标,它是项目实施过程中的一项重要工作。

监控风险实际上是监视项目的进展和项目环境,即项目持续的变化,如图 5-13 所示。其目的是核对风险管理策略和措施的实际效果是否与预见的相同,寻找机会发送和细化风险规避计划,获取反馈信息,以便将来的决策更符合实际。

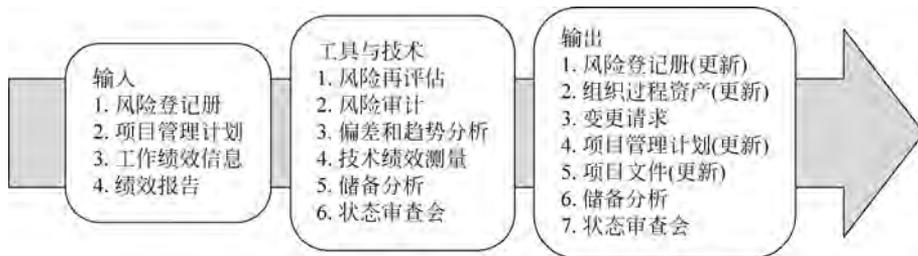


图 5-13 监控风险：输入、工具与技术、输出

在风险监控过程中,及时发现那些新出现的以及预先制定的策略或措施不见效或性质随着时间的推延而发生变化的风险,然后及时反馈,并根据对项目的影响程度,重新进行风险规划、识别、估计、评价和应对,同时还应对每一风险事件制定成败标准和判据。应该在项目生命周期中实施项目管理计划中所列的风险应对措施,还应该持续监督项目工作以便发现新风险、风险变化以及过时的风险。

监控风险过程需要采用诸如偏差和趋势分析的各种技术,这些技术需要以项目实施中生成的绩效信息为基础,监控风险过程的其他目的在于确定:

- (1) 项目的假设条件是否仍然成立。
- (2) 某个已评估过的风险是否发生了变化或已经消失。
- (3) 风险管理政策和程序是否已得到遵守。
- (4) 根据当前的风险评估是否需要调整成本或进度应急储备。



视频讲解

监控风险可能涉及选择替代策略、实施应急或弹回计划、采取纠正措施,以及修订项目管理计划。风险应对责任人应定期向项目经理汇报计划的有效性、未曾预料到的后果,以及为合理应对风险所需采取的纠正措施,在监控风险过程中,还应更新组织过程资产(如项目经验教训数据库和风险管理模板)以使未来的项目受益。

监控风险的数据流向图如图 5-14 所示。

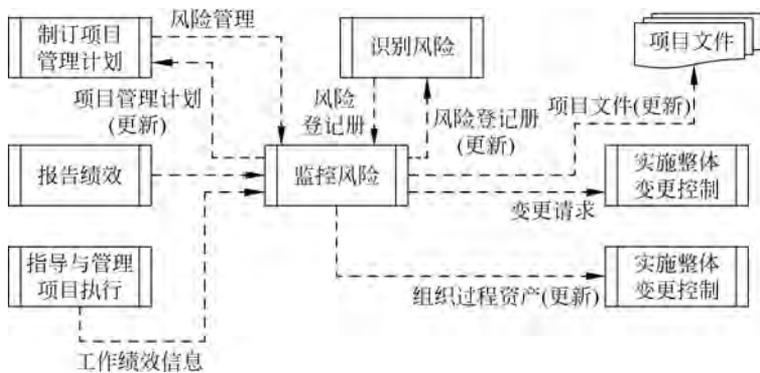


图 5-14 监控风险的数据流向图



视频讲解

## 5.7 案例研究：风险管理实践

### 5.7.1 公司背景简介

湖北 K-E 会计师事务所是湖北省财政厅对国有大中型企业进行社会审计的试点所,承担省直大中型企业的审计工作,具有丰富的工作经验,拥有一批具有丰富实践经验的注册会计师。

湖北省某研究所是省直科研单位,现有 50 多位员工。在基于 Windows 平台开发软件方面,具备较丰富的实战技能。湖北 K-E 会计师事务所在审计工作中发现,很多企业都采用了会计电算化软件,对审计工作提出新的要求。由于社会审计工作的需要,对开发计算机辅助审计软件的愿望越来越强烈,所以就联合湖北省某研究所进行联合开发。

### 5.7.2 实际项目分析

#### 1. 项目介绍

该系统基于 Windows 和 SQL Server 进行开发,开发工具是 Visual Studio。项目开发过程中,共生成程序源代码数万行,项目开发的难度和源代码行数都比预计的要多。计算机辅助审计软件具有工作底稿制作能力和查证功能。数据可传递,能自动生成和人工输入相结合,产生合并抵消分录,能自动产生审计报告和会计报表附注,有灵活开放的系统,方便用户进行二次开发。

#### 2. 开发队伍的风险

开发团队维持在 10 人上下,事务所 3 人,开发单位 6~7 人,有一些人员只能部分时间

工作,开发人员能够自始至终地参加整个项目的工作。开发人员的流动基本能保证工作的连续性。

### 3. 技术风险

数据结构复杂,关联比较多。需要创建新的算法或输入、输出技术,软件需要与其他软件产品的数据库系统接口,客户能确定所要求的功能是可行的。同时,由于当时审计软件在国内的应用尚处于起步阶段,开发人员普遍对该系统比较陌生,这也带来了一定的技术风险。

### 4. 客户相关风险

用户对自己真正的需求并不是十分明确,他们认为计算机是万能的,只要简单地说说自己想干什么就是把需求说明白了,而对业务的规则、工作流程却不愿多谈,也讲不清楚。有的用户日常工作繁忙,他们不愿意付出更多的时间和精力向分析人员讲解业务,这样就加大了分析人员的工作难度和工作量,也可能导致因业务需求不足而使系统风险加大。

### 5. 项目按时完成的风险

另外,这个项目也像许多其他软件项目一样,面临着竣工日期带来的巨大压力。

## 5.7.3 实际的风险管理状况

凭借公司以往的经验,在此软件项目的整个生命周期中,任何阶段都有可能存在风险,工作分解结构(Work Breakdown Structure, WBS)是完整表示项目,且伴随整个项目生命周期的项目要素,如图 5-15 所示。

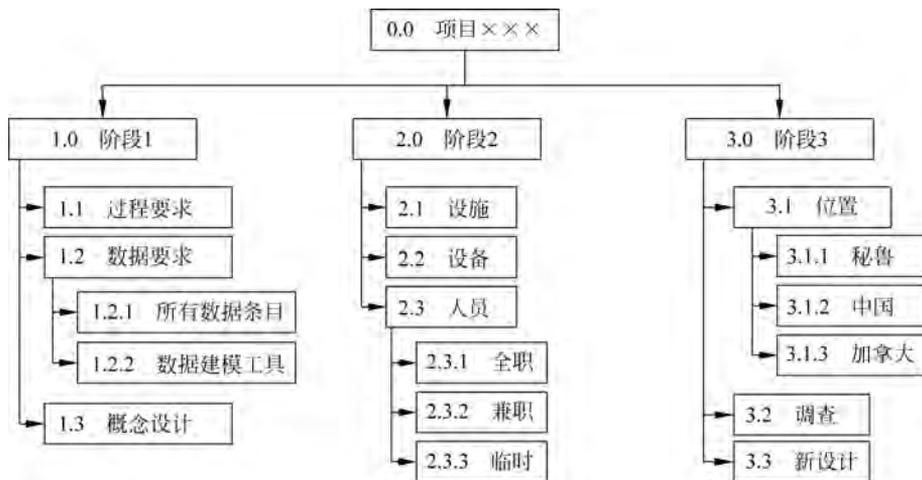


图 5-15 工作分解结构

所以,以 WBS 为基础进行风险管理,既可以方便地识别、标识相应的风险来源,又方便和项目其他工作一起统一管理。在软件项目中各阶段主要工作简述如下。

(1) 启动阶段:进行项目预研,以确定项目是否立项,并对项目的范围进行比较清晰的定义。

(2) 计划编制阶段:进行初步的需求分析,详细定义项目的范围,并对项目涉及的所有

相关活动做尽可能详细的计划。

(3) 执行阶段: 详细分析需求, 保证软件开发生命周期各阶段中不同需求的来源是可追溯的, 并按需求进行设计、编码、测试, 以确定软件产品达到计划给定的范围和标准, 并做相应的部署测试。

(4) 控制阶段: 该阶段贯穿计划和执行两个阶段, 主要进行各种控制, 如需求变更、进度、费用控制, 等等。

(5) 收尾阶段: 项目的收尾工作主要是安装和维护。

在软件开发生命周期的主要阶段中, 通过研究不同阶段的侧重点, 不同的阶段目标以及衡量不同阶段目标的标准, 在软件开发的各个阶段中, 即需求分析阶段、软件设计阶段、编码阶段和测试阶段, 可以发现存在于各阶段中的风险项, 并由项目经理在启动、计划、执行、控制、结束五个阶段予以控制。

### 1. 需求分析阶段

需求分析阶段的风险识别如表 5-4 所示。

表 5-4 需求分析阶段识别的主要风险

阶段目标衡量标准	出现的风险
文字描述的清晰程度	错误理解, 开发错误的软件
需求分析的完整性	系统设计困难、实现的系统与用户需求不一致、测试困难
需求文档的易理解程度	系统设计困难、实现的系统与用户需求不一致、测试困难, 理解错误
需求的稳定性	系统不稳定, 编码困难

需求分析阶段的风险分析如表 5-5 所示。

表 5-5 需求分析阶段风险定性分析

风险项	概率	对本阶段目标的影响力	对其他阶段目标的影响力	对软件开发综合影响力
错误理解需求分析	高	高	高	很高
开发不符合客户需求	一般	高	高	很高
设计困难	一般	一般	高	高
对需求的变动无法做出调整	一般	高	一般	一般
无法在规定时间内完成	高	一般	高	高

需求分析阶段的风险解决如表 5-6 所示。

表 5-6 需求分析阶段风险解决方案

出现的风险项	解决方案
错误理解需求分析	准确规范文字的表达, 必要时召开会议向全体成员介绍需求分析的详细情况, 和客户保持会晤, 采用增量开发模式, 先开发一个基本可以运行的版本, 有利于和客户的交流
开发不符合客户需求的软件	往往是由需求分析的不完备引起的, 可以每周和客户保持会晤, 尽可能细化需求, 以使需求尽可能地完备

续表

出现的风险项	解决方案
下游阶段工作无从下手	对需求文档采用统一的格式,另外,人员之间关系比较重要,该项目组经常进行活动,以培养成员之间的关系。
需求的经常性变更引起的系统不稳定、编码困难、无法及时做出反应、花费时间长、增加成本	计划安排时预先留有余地,另外,对项目开发过程的需求变更严格控制,主要依靠一个需求变更系统进行控制,任何可能影响进度的需求变更都需要经项目经理的认可,项目经理和客户协商后最终决定该变更是否被接受或是延迟到下一版本
无法在规定的时间内完成工作	计划安排的时间预先留有余地,严格按照日程安排完成工作、影响进度的需求变更需要项目经理的认可方被引用,采用增量开发模式,万一项目无法完成,先交付一个替代版本给用户使用,而不至于没有任何东西可以交付

## 2. 设计阶段

设计阶段的风险识别如表 5-7 所示。

表 5-7 设计阶段识别的主要风险

阶段目标的衡量标准	出现的风险
设计报告文字的清晰度	错误理解设计,产生错误的软件
设计的完整性	工作无从下手,功能无法满足需求,编码时间长
设计结构清晰	模块结构中出现错误
设计的复杂性	难度高、更多地关注细节、时间长、对编码人员的要求高
优秀的设计模式	增加设计难度、降低设计效率

设计阶段的风险分析如表 5-8 所示。

表 5-8 设计阶段风险定性分析

风 险 项	概率	对本阶段目标的影响	对其他阶段目标的影响	对软件开发的综合影响
错误理解设计	高	高	高	很高
开发不符合客户要求	一般	低	高	高
下游阶段的工作无从下手	低	低	高	一般
错误的设计结论	一般	高	高	很高
设计复杂性	一般	高	高	很高
无法在规定的时间内完成	低	低	高	高

设计阶段的风险解决如表 5-9 所示。

表 5-9 设计阶段风险解决方案

出现的风险项	解决方案
错误理解设计	准确规范文字的表达,使用统一的设计文档格式,对设计文档的描述方式进行详细的规定,对函数的接口,采用易于理解的代码进行描述,确保不同技术背景的编码人员都能做出准确的理解

续表

出现的风险项	解决方案
开发不符合客户需求的软件	准确规范和具体的文字表达模式,要求设计文档描述尽可能详细,同时项目按模块分为多个小组,各模块的小组长可以随时和编码人员进行沟通
下游阶段工作无从下手	准确规范和具体的文字表达模式,要求设计文档描述尽可能详细,同时项目按模块分为多个小组,各模块的小组长可以随时和编码人员进行沟通
错误的设计结构	尽可能选用技术水平高、经验丰富的人员承担设计任务,鼓励人员在各部门之间流动,有利于集中各个部门的技术骨干解决项目中的困难
设计复杂	与开发人员沟通,必要时进行内部的培训,采用增量的开发模式,划分模块进行设计,逐个解决困难
无法在规定的时间内完成	计划安排预先留有余地,严格按照日程安排完成工作;尽可能选用技术水平高、经验丰富的人员承担设计任务,采用增量的开发模式,交付替代版本,同时保证各个小组之间的并发工作

## 5.7.4 实施效果与总结分析

### 1. 实施效果

此项目开发的目的是为了向审计公司提供辅助审计管理系统。

开发流程也是比较遵从软件工程的规范的。但是最终的结果却不尽如人意,投入了比预计多几倍的人力物力。根据当时参与项目的人员的分析,失败的原因主要如下。

#### 1) 需求不明确

由于出发点和利益不同,系统开发者与用户对于同一问题常有不同看法,这样需求分析的风险就逐渐加大了。另外,对需求变更的控制做得不好,需求的改变就会产生连锁反应,有时候这种反应会导致程序的不稳定。严重的时候,一个错误的修改又引起另一处程序的错误,而新的错误的修改会导致更新的错误。更严重的情况,不是所有的错误都能被修改。

#### 2) 技术风险

此软件数据结构复杂,逻辑关联性比较强。软件需要与第三方财务软件产品的数据库系统接口,带来了开发困难,阻碍了项目的进行。

由于以上原因到了测试阶段,未确定的需求和不断发现的 bug 成了灾难。结果测试当天就因为一个 bug 导致数据被误删和数据混乱。于是暂停测试,改为封闭式开发,并且继续增加人员,第二次修改时才发现整个数据结构也要发生变动,这就无异于重新开发一次,所以最后不得不投入大量的人员予以弥补。

### 2. 分析

分析原因,为什么这个项目会失败?

看来好像是需求没有做好,其实是没有把风险放在整个项目这个大系统下来对待,没有建立一套完整的风险管理机制,这样一来,风险因素就容易被忽略。然而,软件项目前一阶段的失误会对下一阶段产生严重的影响。一旦发生了变化,就不得不修改设计、重写代码、修改测试用例、调整项目计划等,为项目的正常进展带来不尽的麻烦。

所以,没有切实可行的风险管理过程机制,就很难有效地保证风险管理活动的效率。建

立切实可行的风险管理过程机制是软件风险管理理论研究成果最终在实践中得到应用的最根本保证。

## 小结

本章论述了风险及风险管理的概念,介绍了软件风险是导致软件项目进度延迟、预算超支、项目部分或整体失败的因素,以及不确定性和损失时风险的两大属性。软件项目是即将或正在进行的生产过程,既然是未来的事情,就要在项目计划中确定项目的进度、预算和采用的技术等。

风险是伴随软件项目过程而产生的,在软件项目中必须进行风险管理。软件项目的风险管理是一个不断识别风险、分析风险、应对风险及风险监控的过程。

项目风险指可能导致项目损失的不确定性,为某一事件发生给项目目标带来不利影响的可能性。项目风险管理为了最好地达到项目的目标,识别、分配、应对项目生命周期内的风险的科学与艺术,是一种综合性的管理活动。项目的风险管理是一个动态的工作过程,在这个过程中,项目风险的各项作业是相互交叉和互相重叠开展和进行的。项目风险识别是项目风险管理的重要环节。若不能准确地识别项目面临的所有潜在风险,就会失去处理这些风险的最佳时机。



视频讲解

## 思考题

1. 简述软件项目存在较大风险的原因。
2. 简述常见风险及其处理措施。
3. 风险管理是一个系统的过程,请阐述该过程应包含的方面及各个阶段的主要任务。
4. 请阐述一个风险计划所应包含的主要任务。
5. 请列举几种识别风险的方法。谈谈你会如何运用各种方法使其效率及有效性最大化。
6. 请结合自身体会,阐述对于风险识别的认识。