第5章 软件需求与风险管理

负责Contoso制药公司“化学制品跟踪系统”的项目管理人员 Dave会见他的首席程序员Helen和首席测试员Ramesh。他们对新项目都很有兴趣，但他们也记得在以前一个称作“药品仿真”的项目中遇到的问题。

“还记得我们直到进入测试时才发现用户对仿真程序的用户界面极为不满意吗？”Helen问道。“我们花了五周时间重新实现，重新测试，我可再不愿玩这样的死亡游戏了。”

“的确是烦人，”Dave附和道。“同样麻烦的是那些用户提出一大堆没人用过的特性，这样的交互导致编码花费了预计时间的三倍，我们是不管好歹，编完了事，简直是废品！”

“我们太匆忙了，以至没有时间写详细的需求说明” Ramesh回忆道。“测试人员有一半的时间都在问程序员怎样才能判断他们的程序工作正常，以便能测试它。可是程序员设计的一些功能根本就不是用户所要求的。”

“特别麻烦的是，要求开发药品仿真的管理者根本没有看需求规格说明就在上面签字确认了。”Dave补充道：“于是我们不断遇到要求新的特性及各种变更，所以工程超期四个月，成本费用超出预算的一倍这也就不足为怪了。若再发生这样的事，我肯定会被解雇了。”

Ramesh建议道：“也许我们应该把在仿真项目中遇到的问题一一列出来以便我们能在化学制品跟踪系统中避免重蹈覆辙。我看了篇关于软件风险管理的文章，上面介绍说我们应指出各种风险并说明了怎样才能避免它们”。

“我可不那样想”Dave坚持道：“我们已从仿真项目学到了不少，我们不会再有那些问题了。这个项目还没有达到需要用风险管理的地步。如果要把我们可能犯的错误都写下来，好像我连怎样做软件项目都不知道似的。我不想要任何消极想法影响项目。我们必须为成功而制定计划。”

正如Dave的最后一句话所反映的那样，软件工程师都是绝对的乐观主义者。我们总是希望我们的下一个项目进行顺利，而忽略以前项目发生的问题。事实却是许多潜在威胁阻碍项目按计划进行。与Dave的想法恰恰相反的是，软件项目管理者必须要明确和控制他们的项目风险，并且要从需求工程的风险开始进行。

所谓风险是可能给项目的成功带来威胁或损失的情况。这种情况还没有发生，也没有带来问题，而你希望它永远不会发生。但这些潜在的问题可能会给项目成本费用、进度安排、技术方面、产品质量及团队工作效率等带来较大的负面影响。而风险管理 —— 一种软件工业的最佳方法 —— 就是在风险给项目带来损失之前，就指明、评估并对风险加以控制。如果不希望发生的事已经发生了，那就不再是风险，而是事实了。只好通过项目事务 (ongoing)状态跟踪和校正过程来处理当前的问题。

正如没有人能确切地预测未来，风险管理也仅是让你采取一些措施尽可能减少潜在问题

发生的可能性或减少其带来的影响。风险管理的意思是在一种担忧转变为危机或实际困难之前处理它。这将提高项目成功的可能性且可减少不可避免的风险造成的损失。对处于个人控制领域之外的风险应由相应层次的管理者来负责。

由于需求说明在软件项目中扮演着一个核心的角色，故精明的项目管理者会在初期就指明与需求相关的风险并积极地控制它们。典型的需求风险包括对需求的误解、不恰当的用户参与、不确定或随意变更项目的范围和目标以及持续变更需求。项目管理者只能通过与客户、或客户代表（如市场人员）的合作来控制需求风险。合作编写需求风险文档，共同制定减轻风险的措施，增强客户与开发人员之间的合作伙伴关系，这在第 2章中已作介绍了。

不仔细研究是不能把风险撵走的，因此本章对需求风险管理进行简略的介绍。本章后面还会提到需求工程中常出现的一些风险因素。运用这些信息可以使你在风险攻击项目前处理风险。

5.1 软件风险管理基础

除了与项目范围和需求有关的风险外，项目还面临着许多风险。依赖于外界实体，例如一个转包承揽者或生产重用部件的另一个项目就是一种常见的风险来源。项目管理一直面临各种风险挑战：不准确的估计、对准确估计的否决、对项目状态不清楚及资金的周转的困难。技术风险威胁着高度复杂或很前沿 (leading-edge)的开发项目，缺乏知识是另一种风险源，以及参与者对所用的技术和应用领域很陌生等等。强制的或总是变更的政府规范会使一个很好的计划彻底作废。

很可怕吧？这就是为什么所有的项目都应该认真地进行风险管理的原因，风险管理是不断察看水平线上是否出现了冰山，而不是以充足的信心认为船不会沉就以全速挺进。注意同其他过程一样，让你的风险管理活动与工程规模相适应。小规模的工程可以只列出一张简单的风险清单，但对于一个大规模项目的成功，正式的风险管理计划则显得非常重要。

5.1.1 风险管理的要素

风险管理就是使用某些工具和步骤把项目风险限制在一个可接受的范围内。风险管理提供了一种标准的方法来指出风险并把风险因素编成文档，评估其潜在的威胁，以及确定减少这些风险的战略（Williams，Walker， and Dorofee 1997）。风险管理包括的活动如图5-1所示。

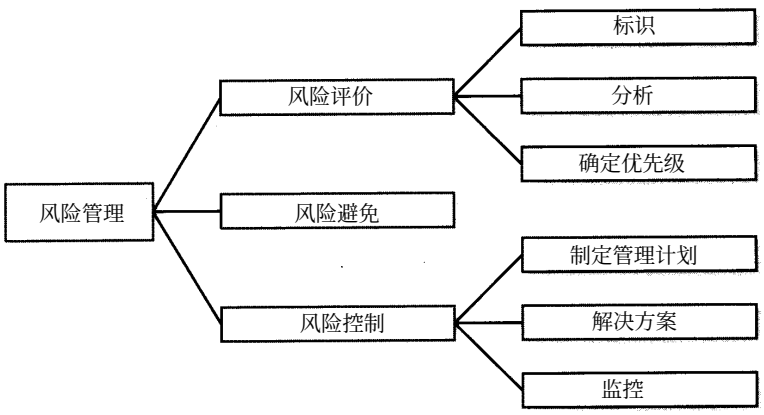

图5-1 风险管理要素

风险评价（risk assessment）是一个检查工程项目并识别潜在风险区域的过程。可以通过

列举通常的软件项目风险因素，如需求风险因素的办法来使风险识别（ risk identification）更加方便容易。本章后面描述了一些需求风险因素（ Carr et al 1993；McConnell 1996）。在风险分析中，应检查一些特定风险对项目可能造成的潜在后果。风险分级（ risk prioritization）有助你通过评价每项风险的潜在危害值，优先处理最严重的风险。风险危害值 (risk exposure)包括带来损失的可能性大小和潜在损失的规模。

风险避免（risk avoidance）是处理风险的一种方法：尽量别作冒险的事。如果你不承担任何项目，采用成熟而并非处于研究阶段的技术，或者将难以实现的特性都排除在项目之外你就可以避开风险。

但更常见的是，需要采取风险控制（ risk control）的方法来管理那些已被发现为高优先级的风险。制定风险管理计划是一项处理具有一旦发生，影响较大的风险的计划，包括降低风险的方法、应急计划、负责人和截止日期。应尽量避免让风险成为真正的问题，或即便问题发生了，也应尽量让其影响降低到最小。风险不能够自我控制，所以风险解决方案就包括了降低、减少每项风险的执行计划。最后，通过风险监控（ risk monitoring）来跟踪风险解决过程的进展情况。这也是例外的项目状态跟踪的一部分内容。监控可以很好了解降低风险工作的进展情况，可以定期地修订先前风险清单的内容和划分的优先级。

5.1.2 编写项目风险文档

仅仅认识到项目面临的风险是远远不够的。应该将其编写成文档并妥善进行管理，这样在整个项目开发过程中有利于风险承担者了解风险情况和状态。图 5-2提供了一个编写一个条目（item）风险说明的模板。你可能觉得以表格形式存放在电子表格中更加方便，因为那样更易于把各项风险进行排序（列表）。但将风险列表(清单)组成一独立文档以便在整个项目中进行升级和维护。

风险条目跟踪模板

序列号：
<顺序号>
确定日期：
<风险被识别出的日期>
撤消日期：
<撤消风险确定日期>
描述：
<以“条件-结果”的形式描述风险>
可能性：
<风险转变为问题的可能性>
影响：
<如果风险变成了事实将造成的损失>
危害值：
<可能性×影响>
降低风险计划：
<一种或多种用来控制、避免、最小化及降低风险的方法>
负责人：
<解决风险的责任承担者>
截止日期：
<完成降低风险措施的截止日期>

图5-2 风险条目跟踪模板

在编写风险说明时，最好采用条件——结果的形式。也就是，先说明你关心的条件，接着是潜在的有害结果（如果风险成为事实）。有时，人们只说明了风险条件（如“客户不同意产品的需求说明”）或者只说明了结果（“我们只能满足某些主要的客户”）。最好将这样的说明句子合并成条件——结果形式的结构：“如果有些客户不赞同产品的需求说明，那我们只能满足某些主要客户的意见。”而一个条件下可能有多个结果，同时也可能出现多个条件下导致同一个结果。

模板能记录风险变为事实的可能性及对项目的消极影响，还有整个的风险危害值（可能性×影响）。我用0.1（极不可能）到1.0（肯定发生）来描述可能性，用1（无甚么影响）到10（有很深、很大的影响）来表示影响。将这两个因素相乘即可作为评估风险危害值的依据。

不要试图精确量化风险。你的目标是将最有威胁的风险和那些不急需处理的风险区别开来。大家可能更愿意用高、中和低来估计可能性及影响。但风险条目中至少应有一个为高的风险。

制定降低风险计划来明确控制风险要采取的活动，其中一些策略是尽量降低风险发生的可能性；而另一些则是减少风险发生后带来的影响。做计划时要考虑降低风险所耗费用，千万别花费20 000美元来控制一项仅会损失10 000美元的风险。为每项风险安排一个负责人，并确定完成活动的截止日期。长期或复杂的风险可能需要具有多个阶段性成果的多步骤降低风险策略计划。

图5-3说明了本章开始部分介绍的“化学制品跟踪系统”小组领导者讨论的一个风险。小组凭他们以前的经验估计了风险的可能性及其影响。除非他们把其它风险因素也估计出来，否则他们并不明白风险危害值4.2究竟有多严重。降低风险措施的前两条是通过更多的用户参与项目来减少风险发生的可能性。而采用原型法则可以利用用户关于界面的早期反馈来减少风险的潜在影响。

5.1.3 制定风险管理计划

一张风险列表还不等于一个风险管理计划。对于一个小项目，你可以把控制风险的计划放在软件项目管理计划里。但一个大项目则需要一份独立的风险管理计划，包括用于识别、评估、编写、跟踪风险的各种方法与途径。这份计划还应包括风险管理活动的角色和责任。你可能希望专门让一个项目风险管理人员负责可能引起麻烦的事。

通常，项目小组为他们的关键活动制定了计划，却在项目中没有按计划去实施或者未能按实际情况进行及时的调整。要坚持按照所采取的风险管理活动计划去执行。项目的进度安排上也应给风险管理留出足够时间来确保项目并未浪费早期投资在风险计划制定上。工程项目的工作分类细目结构中包括降低风险的活动、状态报告，以及更新风险清单。

和其它项目管理活动一样，你需要建立起周期性的监控措施。保持对十来个有最大危害的风险的高度重视，并追踪降低风险措施的有效性。当完成一项活动后，重新评估那项风险的可能性和影响，更新风险清单和其它相关的计划。当控制住原本有很高优先级的风险后，必然有新条目会进入前十条。请记住，不要仅仅因为完成了一项降低风险的活动而人为增加一条风险来进行控制。应当想想你降低风险的方法是否的确减少了风险的危害，使其减少到了一个可以接受的水平。

化学制品跟踪系统的风险条目样例

序列号：
1
确定日期：
5/4/99
撤消日期：

描述：
需求获取中无合适用户参与,导致测试之后用户界面的返工。 .
可能性：
0.6
影响：
7
危害值：
4.2
降低风险计划：
1. 在第一阶段早期就要收集易学、易用的需求。
2. 与产品代表一起召开JAD会议以开发需求。
3. 通过与产品代表和顾问的交流，开发一个包含核心功能的用户界面原型。让产品代表和其他用户来评估此原型。

负责人：
Helen
截止日期：
在6/16/99前完成JAD会议。

图5-3 化学制品跟踪系统的风险条目样例

5.2 与需求有关的风险

下面介绍的风险因素是按需求工程中获取、分析、编写规格说明、验证和管理汇总起来的，并推荐了一些方法用于降低风险发生的可能性或减轻风险发生给项目带来的影响。这张清单仅仅是一个起点，在你做项目逐渐积累经验过程中，加入你的风险因素清单和减轻风险的策略。使用这里提供的条目来帮助你识别需求风险并采用条件 —— 结果的格式来书写风险说明。

5.2.1 需求获取

1) 产品视图与范围　如果团队成员没有对他们要做的产品功能达成一个清晰的共识，则很可能导致项目范围的逐渐扩大。因此最好在项目早期写一份项目视图与范围将业务需求涵盖在内，并将其作为新的需求及修改需求的指导。

2) 需求开发所需时间　紧张的工程进度安排给管理者造成很大的压力，使他们觉得不赶紧开始编码将无法按时完成项目，因而对需求一带而过。项目因其规模和应用种类不同（如信息系统，系统软件，商业的或军事的应用）而有着很大的不同。粗略的统计表明：需求开发工作应占全部工作量的 15%（Rubin 1999）。记录你参与的每个项目中实际需求开发的工作量，这样就能知道所花的时间是否合适并改进将来项目的工作计划。

3) 需求规格说明的完整性和正确性　为确保需求是客户真正需要的，要以用户的任务为中心，应用使用实例技术获取需求。根据不同的使用情景编写需求测试用例，建立原型，使需求对用户来说更加直观，同时获取用户的反馈信息。让客户代表对需求规格说明和分析模型进行正式的评审。

4) 对革新产品的需求　有时容易忽略市场对产品的反馈信息。故要强调市场调查研究，建立原型，并运用客户核心小组来获得革新产品任务的反馈信息。

5) 明确非功能需求　由于一般强调产品的功能性要求，非常容易忽略产品的非功能性的需求。询问客户关于产品性能、使用性、完整性、可靠性等质量特性，编写非功能需求文档和验收标准，（像在SRS中一样）作为可接受的标准。

6) 客户赞同产品需求　如果不同的客户对产品有不同的意见，那最后必将有些客户会不满意。确定出主要的客户，并采用产品代表的方法来确保客户代表的积极参与，确保在需求决定权上有正确的人选。

7) 未加说明的需求　客户可能会有一些隐含的期望要求，但并未说明。要尽量识别并记录这些假设。提出大量的问题来提示客户以充分表达他们的想法、主意和应关注的一切。

8) 把已有的产品作为需求基线　在升级或重做的项目中需求开发可能显得不很重要。开发人员有时被迫把已有的产品作为需求说明的来源。“只是修改一些错误和增加一些新特性”，这时的开发人员不得不通过现有产品的逆向工程 (reverse engineering)来获取需求。可是，逆向工程对收集需求是一种既不充分也不完整的方法。因此新系统很可能会有一些与现有系统同样的缺陷。将在逆向工程中收集的需求编写成文档，并让客户评审以确保其正确性。

9) 给出期望的解决办法　用户推荐的解决方法往往掩盖了用户的实际需求，导致业务处理的低效，或者给开发人员带来压力以至做出很差的设计方案。因此分析人员应尽力从客户叙说的解决方法中提炼出其本质核心。

5.2.2 需求分析

1) 划分需求优先级　划分出每项需求、特性或使用实例的优先级并安排在特定的产品版本或实现步骤中。评估每项新需求的优先级并与已有的工作主体相对比以做出相应的决策。

2) 带来技术困难的特性　分析每项需求的可行性以确定是否能按计划实现。成功好象总是悬于一线的，于是运用项目状态跟踪的办法管理那些落后于计划安排的需求，并尽早采取措施纠正。

3) 不熟悉的技术、方法、语言、工具或硬件平台　不要低估了学习曲线中表明的满足某项需求所需要的新技术的速度跟进情况。明确那些高风险的需求并留出一段充裕时间从错误中学习、实验及测试原型。

5.2.3 需求规格说明

1) 需求理解　开发人员和客户对需求的不同理解会带来彼此间的期望差异，将导致最终产品无法满足客户的要求。对需求文档进行正式评审的团队应包括开发人员，测试人员和客户。训练有素且颇有经验的需求分析人员能通过询问客户一些合适的问题，从而写出更好的规格说明。模型和原型能从不同角度说明需求，这样可使一些模糊的需求变得清晰。

2) 时间压力对TBD的影响　将SRS中需要将来进一步解决的需求注上TBD记号，但如果这

些TBD并未解决，则将给结构设计与项目的继续进行带来很大风险。因此应记录解决每项TBD的负责人的名字，如何解决的以及解决的截止日期。

3) 具有二义性的术语　建立一本术语和数据字典，用于定义所有的业务和技术词汇，以防止它被不同的读者理解为不同的意思。特别是要说明清楚那些既有普通含义又有专用领域含义的词语。对SRS的评审能够帮助参与者对关键术语、概念等达成一致的共识。

4) 需求说明中包括了设计　包含在SRS中的设计方法将对开发人员造成不必要的限制并妨碍他们发挥创造性设计出最佳的方案。仔细评审需求说明以确保它是在强调解决业务问题需要做什么，而不是在说怎么做。

5.2.4 需求验证

1) 未经验证的需求　审查相当篇幅的SRS是有些令人沮丧，正如要在开发过程早期编写测试用例一样。但如果在构造设计开始之前通过验证基于需求的测试计划和原型测试来验证需求的正确性及其质量，就能大大减少项目后期的返工现象。在项目计划中应为这些保证质量的活动预留时间并提供资源。从客户代表方获得参与需求评审的赞同（承诺），并尽早且以尽可能低的成本通过非正式的评审逐渐到正式评审来找出其存在的问题。

2) 审查的有效性　如果评审人员不懂得怎样正确地评审需求文档和怎样做到有效评审，那么很可能会遗留一些严重的问题。故要对参与需求文档评审的所有团队成员进行培训，请组织内部有经验的评审专家或外界的咨询顾问来讲课、授教以使评审工作更加有效。

5.2.5 需求管理

1) 变更需求　将项目视图与范围文档作为变更的参照可以减少项目范围的延伸。用户积极参与的具有良好合作精神的需求获取过程可把需求变更减少近一半（ Jones 1996a）。能在早期发现需求错误的质量控制方法可以减少以后发生变更的可能。而为了减少需求变更的影响，将那些易于变更的需求用多种方案实现，并在设计时更要注重其可修改性。

2) 需求变更过程　需求变更的风险来源于未曾明确的变更过程或采用的变动机制无效或不按计划的过程来做出变更。应当在开发的各阶层都建立变更管理的纪律和氛围，当然这需要时间。需求变更过程包括对变更的影响评估，提供决策的变更控制委员会，以及支持确定重要起点步骤的工具。

3) 未实现的需求　需求跟踪能力矩阵有助于避免在设计、结构建立及测试期间遗漏的任何需求。也有助于确保不会因为交流不充分而导致多个开发人员都未实现某项需求。

4) 扩充项目范围　如果开始未很好定义需求，那么很可能隔段时间就要扩充项目的范围。产品中未说明白的地方将耗费比预料中更多的工作量，而且按最初需求所分配好的项目资源也可能不按实际更改后用户的需求而调整。为减少这些风险，要对阶段递增式的生存期制定计划，在早期版本中实现核心功能，并在以后的阶段中逐步增加实现需求。

5.3 风险管理是你的好助手

项目管理人员可以运用风险管理来提高对造成项目损失的条件的警惕，在需求获取阶段要有用户的积极参与。精明的管理者不仅能认识到它能带来风险的条件，而且将它编入风险清单，并依据以往项目的经验估计其可能性和影响。如果用户一直没有参与，风险危害值将

会扩大以至危害项目的成功。我曾说服管理人员把项目延期是由于缺少用户的积极参与，我告诉他们不能把公司的资金投入一项注定要失败的项目。

周期性的风险跟踪能使管理人员保持对风险危害变化的了解，对那些并未得到完全控制的风险能得到高层管理人员的注意。他们要么开始采取一些修正措施，要么不管风险，依旧按原业务决策思路进行。即使不能控制项目可能遇到的所有风险，风险管理也能使你看清形势，做出的决策是有所依据。

下一步：

- 明确你当前项目面临的一些与需求有关的风险，不要把当前的问题当作风险，一定要是那些还未发生的事情。将风险因素用条件——结果形式编写成文档， 正如图5-2模板所示的那样。为每项风险推荐至少一种可能的降低风险的方法。
- 召集代表开发、市场、客户和管理各方面的风险承担者召开风险“集体研讨”会议。尽力找出更多与需求有关的风险因素。估计每项风险发生的可能性及其影响，两者乘积就是风险危害值。通过按风险危害值降序排列找到最高的五项风险。为每项风险安排一个负责人负责实施降低风险的活动。