28 Gestão de Riscos

Conceitos-Chave

Em seu livro sobre análise e gestão de riscos, Robert Charette [Cha89] apresenta uma definição conceitual de risco:

> Primeiro, o risco refere-se a acontecimentos futuros. Hoje e ontem já não constituem mais uma preocupação, já que estamos colhendo os resultados de nossas ações. A pergunta é, mudando nossas ações hoje, podemos, então, criar uma oportunidade para uma situação diferente e, conforme esperamos, melhor para nós mesmos amanhã? Segundo, isso significa que o risco envolve mudanças, como de opinião, ações ou lugares... [Terceiro,] o risco envolve escolha e a incerteza que a própria escolha traz. Paradoxalmente, o risco, assim como a morte e os impostos, é uma das poucas certezas da vida.

Quando se considera risco no contexto da engenharia de software, os três fundamentos conceituais de Charette estão sempre em evidência. O futuro é uma preocupação — quais riscos podem fazer o projeto de software dar errado? A alteração é uma preocupação — como as alterações nos requisitos do cliente, nas tecnologias de desenvolvimento, nos ambientes-alvo e todas as outras entidades conectadas ao projeto afetam a cadência e o sucesso geral? Por último, deve-se levar a sério as escolhas — que métodos e ferramentas deve-se usar, quantas pessoas deverão ser envolvidas, quanta ênfase na qualidade seria "suficiente"?

Peter Drucker [Dru75] disse certa vez, "Embora seja tolice querer eliminar o risco, e é questionável tentar minimizá-lo, é essencial que os riscos assumidos sejam os certos". Para que você possa identificar os "riscos certos" a ser assumidos durante um projeto de software, é importante identificar todos os riscos óbvios tanto para os gerentes quanto para os profissionais.

Panorama

O que é? Análise e gestão de risco são ações que ajudam uma equipe de software a entender e gerenciar a incerteza. Muitos problemas podem perturbar um projeto de software. O risco é um problema potencial — ele pode ocorrer ou não. Independentemente do resultado, é aconselhável identificá-lo, avaliar sua probabilidade de ocorrência, estimar seu impacto e estabelecer um plano de contingência caso o problema realmente ocorra.

Quem realiza? Todos aqueles envolvidos na gestão de qualidade — gerentes, engenheiros de software e outros interessados — participam da análise e gestão do risco.

Por que é importante? Pense naquele princípio dos escoteiros: "Sempre alerta". Software é uma empreitada difícil. Muitas coisas podem dar errado, e, francamente, muitas vezes dão. Por essa razão, estar preparado — entender os riscos e tomar medidas proativas para evitá-los ou administrá-los — é um elemento-chave do bom gerenciamento de projeto de software.

Quais são as etapas envolvidas? Reconhecer o que pode dar errado é o primeiro passo, chamado de "identificação do risco". Em seguida, o risco é analisado para determinar a probabilidade de que ocorra e o dano que causará, se ocorrer. Uma vez estabelecidas essas informações, os riscos são classificados, por probabilidade e por impacto. Por fim, é desenvolvido um plano para gerenciar os riscos de alta probabilidade e alto impacto.

Qual é o artefato? É produzido um plano de mitigação, monitoramento e gestão de risco (*risk mitigation, monitoring, and management — RMMM*) ou um conjunto de formulários de informações sobre o risco.

Como garantir que o trabalho foi realizado corretamente? Os riscos analisados e gerenciados serão resultantes de um estudo completo das pessoas, produto, processo e projeto. O RMMM deverá ser sempre examinado na medida em que o projeto avança para garantir que os riscos se mantenham atualizados. Os planos de contingência para gerenciamento de risco deverão ser realistas.

28.1 Estratégias de Riscos Reativa *versus* Proativa

"Se você não atacar os riscos ativamente, eles ativamente atacarão você."

Tom Gilb

Estratégias de risco *reativas* têm sido chamadas de forma pejorativa como "Escola Indiana Jones de gestão de risco" [Tho92]. Nos filmes que levam seu nome, Indiana Jones, ao enfrentar uma enorme dificuldade, invariavelmente diria, "Não se preocupe, vou pensar em alguma coisa!". Nunca se preocupe com os problemas até eles acontecerem, Indy reagiria de alguma forma heroica.

Infelizmente, o gerente de projeto de software não é um Indiana Jones, e os membros de sua equipe de projeto de software não são seus fiéis seguidores. No entanto, a maioria das equipes de software depende apenas de estratégias de risco reativas. No melhor dos casos, uma estratégia reativa monitora o projeto à procura de riscos prováveis. São reservados recursos para enfrentar os riscos, caso se tornem problemas reais. Normalmente, a equipe de software não faz nada sobre os riscos até que alguma coisa dê errado. Desse modo, a equipe corre na tentativa de corrigir o problema rapidamente. Isso costuma ser chamado de *modo de combate ao incêndio*. Quando falha, os "gestores de crises" [Cha92] assumem, e o projeto está realmente ameaçado.

Uma estratégia consideravelmente mais inteligente para o gerenciamento de risco é ser proativo. Uma estratégia *proativa* inicia muito antes que o trabalho técnico comece. São identificados os riscos potenciais, avalia-se a probabilidade e o impacto, e os riscos são classificados por ordem de importância. Então, a equipe de software estabelece um plano para gerenciar o risco. O objetivo primário é evitar o risco, mas como nem todos os riscos podem ser evitados, o grupo trabalha para desenvolver um plano de contingência que lhe permita responder de maneira controlada e eficaz. Durante todo o restante deste capítulo, discutiremos uma estratégia proativa de gestão de risco.

28.2 Riscos de Software

Embora já se tenha debatido muito sobre a definição apropriada para risco de software, há um consenso geral de que o risco sempre envolve duas características: *incerteza* — o risco pode ou não ocorrer, isto é, não existem riscos com probabilidade de 100%[1] — e *perda* — se o risco se tornar uma realidade, ocorrerão consequências indesejadas ou perdas [Hig95]. Quando os riscos são analisados, é importante quantificar o nível de incerteza e o grau de perda associada a cada risco. Para tanto, consideram-se diferentes categorias de riscos.

? Que tipos de riscos você provavelmente encontrará ao criar software?

Riscos de projeto ameaçam o plano do projeto. Isto é, se os riscos do projeto se tornarem reais, é possível que o cronograma fique atrasado e os custos aumentem. Os riscos de projeto identificam problemas potenciais de orçamento, cronograma, pessoal (equipes e organização), recursos, clientes, e requisitos e seu impacto sobre o projeto de software. No Capítulo 26, a complexidade do projeto, tamanho e grau de incerteza estrutural também foram definidos como fatores de risco de projeto (e de estimativa).

Riscos técnicos ameaçam a qualidade e a data de entrega do software a ser produzido. Se um risco técnico potencial se torna realidade, a implementação pode se tornar difícil ou impossível. Os riscos técnicos identificam problemas potenciais de projeto, implementação, interface, verificação e manutenção. Além disso, a ambiguidade de especificações, a incerteza técnica, a obsolescência técnica e a tecnologia "de ponta" também são fatores de risco. Riscos técnicos ocorrem porque o problema é mais difícil de resolver do que se pensava.

Riscos de negócio ameaçam a viabilidade do software a ser criado e muitas vezes ameaçam o projeto ou o produto. Os candidatos aos cinco principais riscos de negócio são (1) criar um excelente produto ou sistema que ninguém realmente quer (risco de mercado), (2) criar um produto que não se encaixe mais na estratégia geral de negócios da empresa (risco estratégico), (3) criar um produto que a equipe de vendas não sabe como vender (risco de vendas), (4) perda de suporte da alta gerência devido à mudança no foco ou mudança de profissionais (risco gerencial), e (5) perda do orçamento ou do comprometimento dos profissionais (riscos de orçamento).

---

1 Um risco 100% provável é uma restrição no projeto de software.

"Projetos sem nenhum risco real são fracassos. Eles são quase sempre desprovidos de benefícios; e é por essa razão que não foram feitos anos atrás."

Tom DeMarco e Tim Lister

É extremamente importante observar que uma simples classificação de risco nem sempre funcionará. Alguns riscos são impossíveis de prever.

Uma outra classificação geral dos riscos foi proposta por Charette [Cha89]. *Riscos conhecidos* são aqueles que podem ser descobertos após uma cuidadosa avaliação do plano do projeto, do ambiente comercial e técnico no qual o projeto está sendo desenvolvido e de outras fontes de informação confiáveis (por exemplo, data de entrega irreal, falta de documentação dos requisitos ou do escopo do software, ambiente de desenvolvimento ruim). *Riscos previsíveis* são extrapolados da experiência de projetos anteriores (por exemplo, rotatividade do pessoal, comunicação deficiente com o cliente, diluição do esforço da equipe conforme as solicitações de manutenção vão sendo atendidas). *Erros imprevisíveis* são o curinga no baralho. Eles podem ou não ocorrer, mas são extremamente difíceis de identificar com antecedência.

INFORMAÇÕES

Sete princípios da gestão de risco

O Instituto de Engenharia de Software (Software Engineering Institute — SEI) (**www.sei.cmu.edu**) identifica sete princípios que "proporcionam uma estrutura para conseguir uma gestão de risco eficaz". São eles:

Mantenha uma perspectiva global — encare os riscos de software sob o contexto de um sistema no qual ele é um componente e o problema de negócio que se pretende resolver.

Tenha uma visão antecipada — pense sobre os riscos que podem surgir no futuro (por exemplo, devido a mudanças no software); estabeleça planos de contingência para que os eventos futuros sejam controláveis.

Estimule a comunicação aberta — se alguém apontar um risco potencial, não menospreze. Se um risco é proposto de uma maneira informal, considere-o. Estimule todos os interessados e usuários a sugerir riscos em qualquer instante.

Integre — uma consideração do risco deve ser integrada na gestão de qualidade.

Enfatize um processo contínuo — a equipe deve estar vigilante por toda a gestão de qualidade, modificando os riscos identificados na medida em que mais informações forem conhecidas e acrescentando novos quando uma visão melhor é obtida.

Desenvolva uma visão compartilhada do produto — se todos os interessados compartilham da mesma visão do software, é provável que se tenha uma melhor identificação e avaliação do risco.

Estimule o trabalho de equipe — os talentos, habilidades e conhecimento de todos os interessados deverão ser examinados quando se executam atividades de gestão de risco.

28.3 IDENTIFICAÇÃO DO RISCO

A identificação do risco é uma tentativa sistemática para especificar ameaças ao plano do projeto (estimativas, cronograma, recursos etc.). Identificando os riscos conhecidos e previsíveis, o gerente de projeto dá o primeiro passo no sentido de evitá-los quando possível e controlá-los quando necessário.

AVISO

Embora seja importante considerar os riscos genéricos, são os riscos específicos do produto que causam os maiores problemas. Dedique tempo suficiente para identificar tantos riscos de produto quanto for possível.

Há dois tipos distintos de riscos para cada uma das categorias apresentadas na Seção 28.2: riscos genéricos e riscos específicos de produto. *Riscos genéricos* é uma ameaça potencial a todo projeto de software. *Riscos específicos de produto* podem ser identificados somente por aqueles que têm uma visão clara da tecnologia, das pessoas e do ambiente específico para o qual o software está sendo desenvolvido. Para identificar riscos específicos de produto, são examinados o plano do projeto e a definição de escopo do projeto, e procura-se uma resposta para a seguinte pergunta: "Que características especiais desse produto podem ameaçar o plano do nosso projeto?".

Um método para identificar riscos é criar uma *checklist* (lista de verificação) dos itens de risco. Ela pode ser usada para identificação do risco e concentra-se em alguns dos subconjuntos dos riscos conhecidos e previsíveis nas seguintes subcategorias genéricas:

- *Tamanho do produto* — riscos associados ao tamanho geral do software a ser criado ou modificado.
- *Impacto de negócio* — riscos associados a restrições impostas pela gerência ou pelo mercado.

- *Características do cliente* — são riscos associados à sofisticação dos clientes e à habilidade do desenvolvedor em se comunicar com os interessados a tempo.
- *Definição do processo* — riscos associados ao grau em que a gestão de qualidade foi definida e é seguida pela organização de desenvolvimento.
- *Ambiente de desenvolvimento* — riscos associados à disponibilidade e qualidade das ferramentas a ser usadas para criar o produto.
- *Tecnologia a ser criada* — riscos associados à complexidade do sistema a ser criado e com a "novidade" da tecnologia que está embutida no sistema.
- *Quantidade de pessoas e experiência* — riscos associados à experiência técnica em geral e de projeto dos engenheiros de software que farão o trabalho.

A lista dos itens de risco pode ser organizada de diversas maneiras. Questões relevantes a cada um dos tópicos podem ser respondidas para cada projeto de software. As respostas a essas questões permitem estimar o impacto do risco. Um outro formato de lista de itens de risco simplesmente lista as características relevantes a cada subcategoria genérica. Por fim, é listado um conjunto de "componentes e fatores de risco" [AFC88] com sua probabilidade de ocorrência. Fatores de desempenho, suporte, custo e cronograma são discutidos em resposta às últimas questões.

Há disponível na Web muitas listas abrangentes para riscos de projeto de software (por exemplo, [Baa07], [NAS07], [Wor04]). Você pode usá-las para ter uma visão dos riscos genéricos para projetos de software.

28.3.1 Avaliando o risco geral do projeto

As seguintes questões foram derivadas dos dados de risco obtidos entrevistando gerentes de projeto de software experientes em diversas partes do mundo [Kei98]. As questões estão ordenadas por sua importância relativa ao sucesso de um projeto.

? O projeto de software em que estamos trabalhando está em sério risco?

1. A alta gerência e o cliente estão formalmente comprometidos em apoiar o projeto?
2. Os usuários finais estão bastante comprometidos com o projeto e sistema/produto a ser criado?
3. Os requisitos estão amplamente entendidos pela equipe de engenharia de software e seus clientes?
4. Os clientes foram envolvidos totalmente na definição dos requisitos?
5. Os usuários finais têm expectativas realísticas?
6. O escopo do projeto é estável?
7. A equipe de engenharia de software tem a combinação de aptidões adequadas?
8. Os requisitos de projeto são estáveis?
9. A equipe de projeto tem experiência com a tecnologia a ser implementada?
10. O número de pessoas na equipe de projeto é adequado para o trabalho?
11. Todos os clientes e usuários concordam com a importância do projeto e requisitos para o sistema/produto a ser criado?

WebRef

Risk radar (radar de risco) é uma base de dados e ferramentas que ajudam os gerentes a identificar, classificar e comunicar riscos do projeto. Ela pode ser encontrada no site **www.spmn.com**.

Se alguma dessas questões for respondida negativamente, devem ser providenciados, imediatamente, processos de mitigação, monitoração e gerenciamento. O grau de risco do projeto é diretamente proporcional ao número de respostas negativas a essas questões.

28.3.2 Componentes e fatores de risco

A Força Aérea Americana [AFC88] publicou um panfleto contendo excelentes diretrizes para identificação e combate a riscos de software. A abordagem da Força Aérea requer que o gerente de projeto identifique os fatores de risco que afetam os componentes de risco de software —

desempenho, custo, suporte e cronograma. No contexto dessa discussão, os componentes de risco são definidos da seguinte maneira:

"Gerenciamento de risco é gerenciamento de projeto para adultos."
Tim Lister

- *Risco de desempenho* — é o grau de incerteza de que o produto atenderá aos seus requisitos e será adequado para o uso que se pretende.
- *Risco de custo* — é o grau de incerteza de que o orçamento do projeto será mantido.
- *Risco de suporte* — é o grau de incerteza de que o software resultante será fácil de corrigir, adaptar e melhorar.
- *Risco de cronograma* — é o grau de incerteza de que o cronograma do projeto será mantido e que o produto será entregue a tempo.

O impacto de cada motivador de risco sobre o componente de risco é dividido em uma dentre quatro categorias de impacto-negligenciável, marginal, crítico ou catastrófico. Na Figura 28.1 [Boe89], descreve-se uma caracterização das consequências potenciais dos erros (linhas com o título 1) ou falha em obter um resultado desejado (linhas com o título 2).

A categoria de impacto é escolhida com base na caracterização que melhor se adapta à descrição na tabela.

28.4 PREVISÃO DE RISCO

A previsão de risco, também chamada de *estimativa de risco,* tenta classificar cada risco de duas maneiras — (1) a possibilidade ou probabilidade de que o risco seja real e (2) as consequências

FIGURA 28.1
Avaliação de impacto
***Fonte:* (Boe89)**

Componentes / Categoria		Desempenho	Suporte	Custo	Cronograma
Catastrófico	1	Falha em satisfazer o requisito resultaria em falha do missão		A falha resulta em aumento de custo e atrasos no cronograma com valores previstos que excedem $ 500 mil	
	2	Degradação significativa até não cumprimento do desempenho técnico	Software que não responde com agilidade ou que é difícil de dar suporte	Dificuldades financeiras significativas, provável estouro no orçamento	Data de entrega não exequível
Crítico	1	Falha em atender o requisito degradará o desempenho do sistema até um ponto no qual o sucesso da missão é questionável		Falha resulta em atrasos operacionais e/ou aumento de custos com valores estimados entre $ 100 mil e $ 500mil	
	2	Alguma redução no desempenho técnico	Pequenos atrasos nas modificações de software	Alguma falta de recursos financeiros, possíveis estouros de orçamento	Possível atraso na data de entrega
Marginal	1	Falha em atender o requisito resultaria na degradação de missão secundária		Custos, impactos e/ou atrasos de cronograma recuperáveis com valores estimados de $ 1 mil a $ 100 mil	
	2	De mínima a pequena redução no desempenho técnico	Suporte responsivo de software	Recursos financeiros suficientes	Cronograma realístico e possível
Negligenciável	1	Falha em atingir o requisito criaria inconveniência ou impacto não operacional		Erro resulta em pequeno impacto no custo e/ou cronograma com valor esperado de menos de $ 1 mil	
	2	Nenhuma redução do desempenho técnico	Software facilmente suportável	Possível sobra no orçamento	Data de entrega pode ser antecipada

Notas: (1) Potencial consequência de erros ou falhas de software não detectadas.
(2) Potencial consequência se o resultado desejado não é obtido.

dos problemas associados ao risco, caso ele ocorra. Você trabalha com outros gerentes e pessoal técnico para executar quatro etapas de projeção de risco:

1. Estabeleça uma escala que reflita a possibilidade detectada de um risco.
2. Esboce as consequências do risco.
3. Estime o impacto do risco sobre o projeto e o produto.
4. Avalie a exatidão geral da projeção de risco para que não haja mal-entendidos.

Pense seriamente sobre o software que você vai criar e pergunte a si mesmo, "o que pode sair errado?". Crie sua lista e peça a outros membros da equipe que façam o mesmo.

A finalidade dessas etapas é considerar os riscos de uma maneira que leve à definição de prioridades. Nenhuma equipe de software tem os recursos para resolver todos os riscos possíveis com o mesmo grau de rigor. Priorizando os riscos, você pode alocar recursos onde eles terão maior impacto.

28.4.1 Desenvolvendo uma tabela de risco

Uma tabela de riscos lhe fornece uma técnica simples para a projeção de risco.[2] Um exemplo é apresentado na Figura 28.2.

Inicia-se listando todos os riscos (não importa quão remotos sejam) na primeira coluna da tabela. Isso pode ser conseguido com a ajuda da lista de itens de risco mencionada na Seção 28.3. Cada risco é caracterizado na segunda coluna (por exemplo, PS implica risco de tamanho de projeto, BU implica risco de negócio). A probabilidade de cada risco é colocada na próxima coluna da tabela. O valor da probabilidade para cada risco pode ser estimado pelos membros da equipe individualmente. Para tanto, pode-se consultar os membros da equipe em ordem aleatória até que suas avaliações coletivas de risco comecem a convergir.

FIGURA 28.2

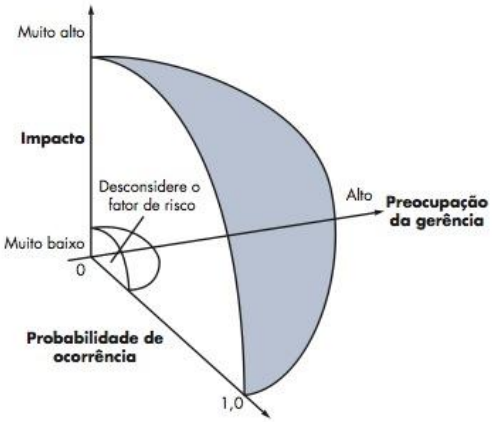
Exemplo de uma tabela de risco antes da ordenação

Riscos	Categoria	Probabilidade	Impacto	RMMM
A estimativa de tamanho pode ser significativamente baixa	PS	60%	2	
Número de usuários maior do que o planejado	PS	30%	3	
Reutilização menor do que a planejada	PS	70%	2	
Os usuários finais resistem ao sistema	BU	40%	3	
O prazo de entrega será apertado	BU	50%	2	
Financiamento será perdido	CU	40%	1	
O cliente mudará os requisitos	PS	80%	2	
A tecnologia não atingirá as expectativas	TE	30%	1	
Falta de treinamento no uso das ferramentas	DE	80%	3	
Pessoal sem experiência	ST	30%	2	
A rotatividade do pessoal será alta	ST	60%	2	
Σ				
Σ				
Σ				

Valores de impacto:
1 — catastrófico
2 — crítico
3 — marginal
4 — negligenciável

2 A tabela de risco pode ser implementada como um modelo de planilha. Isso permite fácil manipulação e ordenação dos valores.

FIGURA 28.3
Riscos e preocupação da gerência



Em seguida, avalia-se o impacto de cada risco. É investigado cada componente de risco usando a caracterização apresentada na Figura 28.1, e determina-se uma categoria de impacto. São tomadas as médias das categorias de cada um dos quatro componentes de risco-desempenho, suporte, custo e cronograma[3] para determinar um valor de impacto global.

PONTO-CHAVE
A tabela de riscos é ordenada por probabilidade e impacto para classificar os riscos.

Uma vez completadas as quatro primeiras colunas da tabela, ela é ordenada por probabilidade e por impacto. Riscos de alta probabilidade, alto impacto se situam no topo da tabela, e riscos de baixa probabilidade posicionam-se no fim. Com isso se completa a priorização de risco de primeira ordem.

Você pode estudar a tabela resultante e definir uma linha de corte (traçada horizontalmente em algum ponto na tabela), que implica que somente riscos que ficam acima da linha receberão mais atenção. Riscos que se posicionam abaixo da linha são reavaliados para uma priorização de segunda ordem. De acordo com a Figura 28.3, o impacto e a probabilidade do risco têm influência distinta na preocupação do gerente. Um fator de risco com alto impacto, mas uma probabilidade de ocorrência muito baixa, não deve absorver tempo significativo da gerência. No entanto, riscos de alto impacto com probabilidade entre moderada e alta e riscos de baixo impacto com alta probabilidade devem ser encaminhados para as etapas de análise de risco a seguir.

"[Hoje] ninguém se dá ao luxo de conhecer uma tarefa tão bem que não possa ter surpresas, e surpresa significa risco."
Stephen Grey

Todos os riscos que ficam acima da linha de corte deverão ser gerenciados. A coluna com o título RMMM contém um ponteiro que aponta para um plano de *mitigação, monitoramento, e gestão do risco* ou, como alternativa, uma coleção de formulários de informações desenvolvida para todos os riscos que se posicionam acima da linha de corte. O plano RMMM e os formulários de informações de risco são discutidos nas Seções 28.5 e 28.6.

A probabilidade do risco pode ser determinada por meio de estimativas individuais e depois pelo desenvolvimento de um valor de consenso. Apesar de essa abordagem funcionar, foram desenvolvidas técnicas mais sofisticadas para determinar a probabilidade do risco [AFC88]. Os fatores de risco podem ser avaliados em uma escala qualitativa de probabilidades que tem os seguintes valores: impossível, improvável, provável e frequente. A probabilidade matemática pode ser associada a cada valor qualitativo (por exemplo, uma probabilidade de 0,7 a 0,99 envolve um risco altamente provável).

3 Pode ser usada uma média ponderada se um componente de risco tiver mais significado para um projeto.

28.4.2 Avaliando o impacto do risco

Três fatores afetam as consequências prováveis se ocorrer um risco: sua natureza, seu escopo e sua época. A natureza do risco indica os problemas que podem surgir se ele ocorrer. Por exemplo, uma interface externa para o hardware do cliente mal definida (um risco técnico) logo atrapalhará o início do projeto e os testes, e provavelmente causará problemas na integração do sistema no fim do projeto. O escopo de um risco relaciona a severidade (quão sério é ele?) com sua distribuição geral (quanto do projeto será afetado ou quantos clientes serão prejudicados?). Por fim, a época do risco considera quando e por quanto tempo o impacto será sentido. Em muitos casos, você vai querer que as "más notícias" ocorram o mais cedo possível, mas em alguns, quanto mais tarde, melhor.

Como avaliamos as consequências de um risco?

Retornando mais uma vez à abordagem de análise de risco proposta pela Força Aérea norte-americana [AFC88], podem-se aplicar os seguintes procedimentos para determinar as consequências gerais de um risco: (1) determinar o valor médio da probabilidade de ocorrência para cada componente de risco; (2) usando a Figura 28.1, determinar o impacto para cada componente com base no critério mostrado, e (3) completar a tabela de risco e analisar os resultados conforme descrito nas seções anteriores.

A exposição geral ao risco (*risk exposure* — RE) é determinada por meio da seguinte relação [Hal98]:

$$\text{RE} = P \times C$$

em que P é a probabilidade de ocorrência de um risco, e C o custo para o projeto, caso o risco ocorra.

Por exemplo, suponha que a equipe de software defina o risco de um projeto da seguinte maneira:

Identificação do risco. Somente 70% dos componentes de software programados para ser reutilizados serão, de fato, integrados na aplicação. A funcionalidade restante terá de ser desenvolvida de forma personalizada.

Probabilidade do risco. 80% (aproximadamente).

Impacto do risco. Foram planejados 60 componentes de software reutilizáveis. Se somente 70% pode ser usado, 18 componentes terão de ser desenvolvidos desde o início (além de outros softwares personalizados que foram planejados para ser desenvolvidos). Pelo fato de cada componente ter em média 100 LOC e os dados locais indicarem que o custo de engenharia de software para cada LOC é de $ 14, o custo total (impacto) para desenvolver os componentes será

$18 \times 100 \times 14 = \$\ 25.200$.

Exposição ao risco. $\text{RE} = 0{,}80 \times 25.200 = \$\ 20.200$.

AVISO

Compare a RE, para todos os riscos, com a estimativa de custos para o projeto. Se RE for maior do que 50% do custo do projeto, a viabilidade do projeto deve ser avaliada.

A exposição ao risco pode ser calculada para cada risco na tabela de riscos, uma vez feita a estimativa do custo do risco. A exposição total para todos os riscos (acima da linha de corte na tabela de riscos) pode proporcionar um meio para ajustar a estimativa final de custo para um projeto. Ela pode também ser usada para prever o aumento provável nos recursos de pessoal necessários em vários pontos durante o cronograma do projeto.

As técnicas de projeção e análise de risco descritas nas Seções 28.4.1 e 28.4.2 são aplicadas iterativamente à medida que avança o projeto de software. A equipe deve rever a tabela de risco a intervalos regulares, reavaliando cada risco para determinar quando novas circunstâncias causam mudanças em probabilidade e impacto. Como uma consequência dessa atividade, pode ser necessário acrescentar novos riscos à tabela, remover alguns que não são mais relevantes e mudar as posições relativas dos que restarem.

CasaSegura

Análise de risco

Cena: Escritório de Doug Miller antes do início do projeto de software *CasaSegura*.

Atores: Doug Miller (gerente da equipe de engenharia de software *do CasaSegura*) e Vinod Raman, Jamie Lazar e outros membros da equipe de engenharia.

Conversa:

Doug: Gostaria de dedicar um tempo para um brainstorming sobre os riscos do projeto *CasaSegura*.

Jamie: E o que pode dar errado?

Doug: Bem. Aqui estão algumas categorias em que as coisas podem dar errado. [Ele mostra a todos as categorias listadas na introdução da Seção 28.3.]

Vinod: Humm... Você quer apenas chamar a nossa atenção para eles, ou...

Doug: Não, veja o que acho que devemos fazer. Cada um faz uma lista de riscos... Agora mesmo..." [Dez minutos para todos escreverem.]

Doug: Ok, parem.

Jamie: Mas eu ainda não terminei!

Doug: Tudo bem. Veremos a lista novamente. Agora, para cada item da sua lista, atribua uma porcentagem de probabilidade de que o risco venha a ocorrer. Depois, atribua um impacto ao projeto em uma escala de 1 (pequeno) a 5 (catastrófico).

Vinod: Se achar que o risco é alto, especifico uma probabilidade de 50%, e se achar que ele tem um impacto moderado sobre o projeto, especifico um 3, certo?

Doug: Exatamente. [Cinco minutos, todos escrevendo.]

Doug: Ok, parem. Agora vamos fazer uma lista de grupos no quadro branco. Eu escrevo; vou pegar um item por vez de cada lista de vocês em uma sequência de rodadas. [Quinze minutos depois, a lista está criada.]

Jamie (apontando para o quadro e rindo): Vinod, aquele risco (apontando para um item do quadro) é ridículo. É mais fácil sermos atingidos por um raio. Deveríamos removê-lo.

Doug: Não, vamos deixar por enquanto. Consideraremos todos os riscos, não importa que sejam absurdos. Depois, vamos limpar a lista.

Jamie: Mas já temos mais de 40 riscos... Como poderemos controlar todos eles?

Doug: Não podemos. É por esse motivo que definiremos um ponto de corte após ordenarmos todos os riscos. Farei isso depois, e nos reunimos amanhã novamente. Por ora, voltemos ao trabalho... E, nos intervalos de folga, pensem sobre quaisquer riscos que tenham esquecido.

28.5 Refinamento do Risco

Durante os primeiros estágios do planejamento de projeto, um risco pode ser especificado de maneira bem generalizada. Conforme o tempo passa e se conhece mais sobre o projeto e o risco, pode ser possível refinar o risco em uma série de riscos detalhados. Cada um deles de certa forma mais fácil de mitigar, monitorar e gerenciar.

Qual é uma boa maneira de descrever um risco?

Uma maneira de fazer isso é representar o risco em um formato *condição-transição-consequência* (CTC) [Glu94]. O risco é definido da seguinte maneira:

> Considerando que <condição> então há a preocupação de que (possivelmente) <consequência>.

Usando o formato CTC para o risco de reutilização descrito na Seção 28.4.2, podemos escrever:

> Considerando que todos os componentes de software reutilizáveis devem estar em conformidade com padrões específicos de projeto e que alguns deles não se enquadram nesses padrões, há uma preocupação de que (possivelmente) somente 70% dos módulos que se planejava reutilizar possam realmente ser integrados na montagem do sistema, resultando na necessidade de criar de forma personalizada os 30% restantes dos componentes.

Essa condição geral pode ser refinada da seguinte maneira:

> **Subcondição 1.** Certos componentes reutilizáveis foram desenvolvidos por uma equipe terceirizada que não conhecia os padrões internos de projeto.
>
> **Subcondição 2.** O padrão de projeto para as interfaces de componente não foi completamente estabelecido e pode não estar em conformidade com certos componentes reutilizáveis existentes.
>
> **Subcondição 3.** Certos componentes reutilizáveis foram implementados em uma linguagem não suportada no ambiente em que serão usados.

As consequências associadas com essas subcondições refinadas permanecem as mesmas (30% dos componentes de software devem ser criados de forma personalizada), mas o refinamento ajuda a isolar os riscos subjacentes e pode levar a uma análise e resposta mais fáceis.

28.6 Mitigação, Monitoração e Controle de Riscos (RMMM)

"Se tomo tantas medidas de precaução, é porque não quero dar chance ao azar."

Napoleão

Todas as atividades de análise de risco apresentadas até este ponto têm um único objetivo: ajudar a equipe de projeto no desenvolvimento de uma estratégia para lidar com o risco. Uma estratégia eficaz deve considerar três aspectos: como evitar o risco, como monitorar o risco e como gerenciar o risco e planejar contingência.

Se a equipe de software adota uma abordagem proativa ao risco, evitar o risco é sempre a melhor estratégia. Para tanto, desenvolve-se um plano para *mitigação de risco*. Por exemplo, suponha que a alta rotatividade de pessoal seja o risco r_1 de um projeto. Com base em histórico passado e com a intuição do gerente, a possibilidade l_1 de alta rotatividade seja estimada em 0,70 (70%, um tanto alta) e o impacto x_1 seja projetado como crítico. A alta rotatividade terá um impacto crítico sobre o custo e cronograma do projeto.

Para mitigar esse risco, devemos desenvolver uma estratégia para redução da rotatividade. Entre as providências possíveis a ser tomadas, citamos:

O que podemos fazer para mitigar um risco?

- Reunir-se com o pessoal para determinar as causas da rotatividade (por exemplo, más condições de trabalho, salário baixo, mercado de trabalho competitivo).
- Mitigar as causas que estão sob o seu controle antes do início do projeto.
- Uma vez iniciado o projeto, assumir que a rotatividade acontecerá e desenvolver técnicas para garantir a continuidade quando as pessoas saírem.
- Organizar equipes de projeto para que as informações sobre cada atividade de desenvolvimento sejam amplamente difundidas.
- Definir padrões para os produtos do projeto e estabelecer mecanismos para assegurar que todos os modelos e documentos sejam desenvolvidos a tempo.
- Executar revisões em pares de todo o trabalho (para que mais de uma pessoa esteja "por dentro").
- Designar uma pessoa substituta para cada profissional cujo trabalho seja crítico.

À medida que o projeto avança, começam as atividades de *monitoramento de risco*. O gerente de projeto monitora fatores que podem fornecer uma indicação sobre se o risco está se tornando mais ou menos possível. No caso da alta rotatividade do pessoal, a atitude geral dos membros da equipe baseada nas pressões do projeto, o grau segundo o qual a equipe se tornou coesa, as relações pessoais entre os membros da equipe, problemas em potencial com remuneração e benefícios, e a disponibilidade de empregos dentro e fora da empresa, tudo isso é monitorado.

Além de monitorar esses fatores, um gerente de projeto deve monitorar a efetividade das providências para a mitigação do risco. Por exemplo, uma providência citada recomendava a definição de padrões para o produto e mecanismos para assegurar que os produtos sejam desenvolvidos a tempo. Esse é um mecanismo para garantir a continuidade, se um elemento crítico deixar o projeto. O gerente de projeto deve monitorar os produtos cuidadosamente para garantir que cada um seja autossuficiente e forneça as informações necessárias se um novato precisar entrar na equipe de software no meio do projeto.

O *gerenciamento de risco e plano de contingência* considera que os esforços de mitigação do risco falharam e que o risco se tornou uma realidade. Continuando o exemplo, o projeto está em andamento e um grupo de pessoas avisa que vai sair. Se a estratégia de mitigação foi utilizada, existe pessoal substituto disponível, as informações estão documentadas e todo o conhecimento compartilhado dentro da equipe. Além disso, pode-se temporariamente mudar o foco dos

recursos (e reajustar o cronograma do projeto) para as funções que estão com o todo o pessoal necessário, permitindo que os novatos a ser acrescentados à equipe "entrem logo no ritmo". As pessoas que estão saindo devem interromper todo o trabalho e passar suas últimas semanas envolvidas em atividades de "transferência de conhecimentos". Isso pode incluir captação de conhecimento por meio de vídeo, desenvolvimento de "documentos de comentário ou Wikis", e/ou reuniões com outros membros da equipe que permanecerão no projeto.

Se a exposição a um risco específico for menor do que seu custo de mitigação, não tente mitigar o risco, mas continue monitorando-o.

É importante observar que as etapas de mitigação, monitoramento e controle de risco (*risk mitigation, monitoring, and management* — RMMM) incorrem em custo adicional no projeto. Por exemplo, o tempo gasto para incluir um substituto para cada técnico essencial custa dinheiro. Parte do gerenciamento de risco é para avaliar quando os benefícios acumulados pelas providências RMMM são superados pelos custos associados a sua implementação. Essencialmente, executa-se uma análise de custo-benefício clássica. Se as providências para evitar os riscos de alta rotatividade aumentarem o custo e duração do projeto em uma estimativa de 15%, mas o fator de custo predominante for o "backup do profissional", o gerente pode decidir não implementar essa etapa. Por outro lado, se houver uma projeção de que as providências para evitar o risco aumentarão os custos em 5% e a duração em apenas 3%, o gerente provavelmente vai tomar essas providências.

Para um grande projeto, 30 ou 40 riscos podem ser identificados. Se para cada um deles forem identificados de 3 a 7 passos de gestão de risco, esta pode se tornar um projeto em si mesma! Por essa razão, deve-se adaptar a regra 80-20 de Pareto para o risco de software. A experiência indica que 80% do risco geral de projeto (80% do potencial de falha do projeto) pode ser responsável por apenas 20% dos riscos identificados. O trabalho executado durante as primeiras etapas de análise de risco o ajudará a determinar quais dos riscos estão incluídos nesses 20% (por exemplo, riscos que levam à maior alta exposição ao risco). Desse modo, alguns dos riscos identificados, avaliados e projetados podem não entrar no plano RMMM — eles não estão incluídos nos 20% críticos (os riscos com prioridade mais alta no projeto).

O risco não está limitado ao próprio projeto de software. Riscos podem ocorrer depois que o software foi desenvolvido com sucesso e entregue ao cliente. Esses riscos estão tipicamente associados às consequências da falha no software em campo.

Segurança do software e análise de imprevistos (por exemplo, [Dun02], [Her00], [Lev95]) são atividades de garantia de qualidade de software (Capítulo 16) que se concentram na identificação e avaliação de imprevistos em potencial que podem afetar negativamente o software e fazer o sistema inteiro falhar. Se imprevistos puderem ser identificados antecipadamente no processo de engenharia de software, características do projeto do software que servirão para eliminar ou controlar os imprevistos em potencial poderão se especificadas.

28.7 O PLANO RMMM

Uma estratégia de gestão de risco pode ser incluída no plano de projeto de software, ou as etapas de gestão de risco podem ser organizadas em um plano de mitigação, monitoração e gerenciamento (RMMM) separado. O plano RMMM documenta todo o trabalho executado como parte da análise de risco e é usado pelo gerente de projeto como parte do plano geral de projeto.

Algumas equipes de software não desenvolvem um documento RMMM formal. Em vez disso, cada risco é documentado individualmente usando-se um *formulário de informações de risco* (*risk information sheet* — (RIS) [Wil97]. Em muitos casos, o RIS é mantido por meio de um sistema de base de dados para que a criação e introdução de informações, ordem de prioridade, pesquisas e outras análises possam ser feitas facilmente. O formato do RIS está ilustrado na Figura 28.4.

Uma vez documentado o RMMM e começado o projeto, iniciam-se as etapas de mitigação e monitoração de risco. Conforme já discutimos, mitigação de risco é uma atividade para evitar problemas. A monitoração de risco é uma atividade de acompanhamento de projeto com três objetivos primários: (1) avaliar se os riscos previstos vão, de fato, ocorrer; (2) assegurar que as

FIGURA 28.4
Formulário de informações de risco
Fonte: [Wil97]

Formulário de informações de risco			
ID do risco: P02-4-32	Data: 09/05/09	Prob: 80%	Impacto: alto
Descrição: Somente 70% dos componentes de software programados para reutilização serão, de fato, integrados na aplicação. A funcionalidade restante terá de ser desenvolvida de maneira personalizada.			
Refinamento/contexto: Subcondição 1: certos componentes reutilizáveis foram desenvolvidos por uma equipe terceirizada que não tinha conhecimento dos padrões de projeto internos. Subcondição 2: o padrão de design para interfaces de componente ainda não foi consolidado e pode não estar em conformidade com certos componentes reutilizáveis. Subcondição 3: certos componentes reutilizáveis foram implementados em uma linguagem não suportada no ambiente a que se destina.			
Mitigação/monitoração: 1. Contate a empresa terceirizada para determinar a conformidade com os padrões de projeto. 2. Pressione para que haja padronização da interface; considere a estrutura de componente ao decidir sobre o protocolo de interface. 3. Determine o número de componentes que estão na categoria da subcondição 3; determine se pode ser adquirido o suporte de linguagem.			
Gerenciamento/plano de contingência/disparo: Foi calculada a exposição ao risco e resultou em $ 20.200. Reserve esse valor no custo de contingência do projeto. Desenvolva um cronograma revisado assumindo que 18 componentes adicionais terão de ser criados de forma personalizada; defina a equipe de maneira correspondente. Disparo: as providências para mitigação improdutivas em 01/07/09.			
Estado atual: 12/05/09: iniciadas as etapas de mitigação.			
Autor: D. Gagne		Autorizado: B. Laster	

etapas de mitigação ao risco definidas para o risco estejam sendo aplicadas adequadamente; e (3) coletar informações que podem ser usadas para futuras análises de riscos. Em muitos casos, os problemas que ocorrem durante um projeto podem estar ligados a mais de um risco. Outra função do monitoramento de risco é tentar definir a origem [quais riscos causaram quais problemas durante o projeto].

FERRAMENTAS DO SOFTWARE

Gestão da qualidade de software

Objetivo: o objetivo das ferramentas de gestão de risco é ajudar a equipe de projeto na definição dos riscos, avaliação de seu impacto e probabilidade, e acompanhamento dos riscos durante todo o projeto de software.

Mecânica: em geral, as ferramentas de gestão de risco ajudam na identificação genérica dos riscos fornecendo uma lista de riscos típicos de projeto e comerciais, proporcionando checklists ou outras técnicas de "entrevista" que ajudam a identificar riscos específicos de projeto, atribuindo probabilidade e impacto a cada risco, suportando estratégias de mitigação de risco e gerando vários relatórios diferentes relacionados aos riscos.

Ferramentas representativas:[4]

@risk, desenvolvida pela Palisade Corporation (**www.palisade.com**), é uma ferramenta genérica de análise de risco que usa simulação de Monte Carlo para controlar seu instrumento analítico.

Riskman, distribuída pela ABS Consulting (**www.absconsulting.com/riskmansoftware/index.html**), é um sistema especializado de avaliação de risco que identifica riscos relacionados com projeto.

Risk Radar, desenvolvida pela SPMN (**www.spmn.com**), auxilia os gerentes de projeto na identificação e gerenciamento de riscos de projeto.

Risk+, desenvolvida pela Deltek (**www.deltek.com**), integra-se com o Microsoft Project para quantificar incerteza de custo e cronograma.

X:PRIMER, desenvolvida pela GrafP Technologies (**www.grafp.com**) é uma ferramenta genérica baseada na Web que prevê o que pode sair errado em um projeto e identifica as principais causas para falhas em potencial e as ações eficazes a tomar.

4 As ferramentas aqui apresentadas não significam um aval, mas, sim, uma amostra dessa categoria. Na maioria dos casos, seus nomes são marcas registradas pelos respectivos desenvolvedores.

28.8 Resumo

Sempre que um projeto de software estiver em execução, o bom senso manda que se faça a análise de risco. No entanto, a maioria dos gerentes de projeto de software a fazem informalmente e superficialmente, quando fazem. O tempo que se gasta identificando, analisando e controlando os riscos oferece retorno de muitas maneiras — menos pressão durante o projeto, uma melhor habilidade para acompanhar e controlar um projeto e a confiança que resulta do planejamento para os problemas antes que eles ocorram.

A análise de riscos pode absorver um volume significativo de trabalho de planejamento do projeto. A identificação, projeção, avaliação, gerenciamento e monitoração, tudo toma tempo. Mas o esforço é recompensado. Citando Sun Tzu, um general chinês que viveu há 2.500 anos, "Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de uma centena de batalhas". Para o gerente de projeto de software, o inimigo é o risco.

Problemas e Pontos a Ponderar

28.1. Forneça cinco exemplos de outros campos que ilustram os problemas associados à estratégia reativa de riscos.

28.2. Descreva a diferença entre "riscos conhecidos" e "riscos previsíveis".

28.3. Acrescente três questões ou tópicos a cada uma das checklists de itens de risco apresentadas no site da SEPA.

28.4. Você foi designado para criar um software que suporte um sistema de edição de vídeo de baixo custo. O sistema aceita como entrada vídeo digital, armazena vídeo em disco e depois permite que o usuário faça uma grande variedade de edições no vídeo digitalizado. O resultado pode então ser gravado em DVD ou outro tipo de mídia. Realize algumas pesquisas sobre sistemas desse tipo e depois faça uma lista dos riscos tecnológicos que enfrentaria ao empreender um projeto desse tipo.

28.5. Você é o gerente de projeto de uma grande empresa de software. Foi designado para liderar uma equipe que está desenvolvendo um software processador de texto "avançado". Crie uma tabela de riscos para o projeto.

28.6. Descreva a diferença entre componentes de risco e fatores de risco.

28.7. Desenvolva uma estratégia de mitigação de risco e especifique atividades específicas de mitigação de risco para três dos riscos descritos na Figura 28.2.

28.8. Desenvolva uma estratégia de monitoração de risco e especifique as atividades de monitoramento de risco para três dos riscos descritos na Figura 28.2. Não se esqueça de identificar os fatores que estará monitorando para determinar se o risco está se tornando mais ou menos possível.

28.9. Desenvolva uma estratégia de gerenciamento de risco e especifique atividades de gerenciamento de risco para três dos riscos descritos na Figura 28.2.

28.10. Tente refinar três dos riscos descritos na Figura 28.2 e depois crie formulários de informações de risco para cada um deles.

28.11. Represente três dos riscos mostrados na Figura 28.2 usando um formato CTC.

28.12. Recalcule a exposição de risco discutida na Seção 28.4.2 quando o custo por LOC é de $ 16 e a probabilidade é de 60%.

28.13. Você pode pensar em uma situação na qual um risco de alta probabilidade e alto impacto não seria considerado como parte do seu plano RMMM?

28.14. Descreva cinco áreas de aplicação de software nas quais a análise de segurança e imprevistos do software seriam uma preocupação importante.

Leituras e Fontes de Informação Complementares

A literatura sobre gestão de risco de software se expandiu significativamente nas últimas décadas. Vun (*Modeling Risk,* Wiley, 2006) dá um tratamento matemático detalhado da análise de risco que pode ser aplicada aos projetos de software. Crohy e seus colegas (*The Essentials of Risk Management,* McGraw-Hill, 2006), Mulcahy (*Risk Management, Tricks of the Trade for Project Managers,* RMC Publications, Inc., 2003), Kendrick (*Identifying and Managing Project Risk,* American Management Association, 2003), e Marrison (*The Fundamentals of Risk Measurement,* McGraw-Hill, 2002) apresentam métodos úteis e ferramentas que todo gerente de projeto pode usar.

DeMarco e Lister (*Dancing with Bears,* Dorset House, 2003) escreveram um livro interessante e esclarecedor que orienta os gerentes e profissionais de software no gerenciamento de riscos. Moynihan (*Coping with IT/IS Risk Management,* Springer-Verlag, 2002) apresenta opiniões pragmáticas de gerentes de projeto que tratam do risco de forma contínua. Royer (*Project Risk Management,* Management Concepts, 2002) e Smith e Merritt (*Proactive Risk Management,* Productivity Press, 2002) sugerem um processo proativo para gestão de risco. Karolak (*Software Engineering Risk Management,* Wiley, 2002) escreveu um guia que introduz um modelo de análise de risco fácil de usar com checklists e questionários suportados por um pacote de software.

Capers Jones (*Assessment and Control of Software Risks,* Prentice Hall, 1994) apresenta uma discussão detalhada dos riscos de software, incluindo dados coletados de centenas de projetos de software. Jones define 60 fatores de risco que podem afetar o resultado dos projetos de software. Boehm [Boe89] sugere um excelente questionário e formatos de checklist que podem ser valiosos na identificação do risco. Charette [Cha89] apresenta uma abordagem detalhada da mecânica da análise de risco, usando teoria de probabilidades e técnicas estatísticas para analisar os riscos. Em outro volume, Charette (*Application Strategies for Risk Analysis,* McGraw-Hill, 1990) discute o risco no contexto de sistema e engenharia de software e sugere estratégias pragmáticas para gestão de risco. Gilb (*Principles of Software Engineering Management,* Addison-Wesley, 1988) apresenta uma série de "princípios" (frequentemente são divertidos e às vezes profundos) que podem servir de excelente guia para gestão de risco.

Ewusi-Mensah (*Software Development Failures: Anatomy of Abandoned Projects,* MIT Press, 2003) e Yourdon (*Death March,* Prentice Hall, 1997) discutem o que acontece quando os riscos engolfam a equipe de projeto de software. Bernstein (*Against the Gods,* Wiley, 1998) apresenta uma história interessante do risco que remonta aos tempos antigos.

O Software Engineering Institute publicou muitos relatórios e guias detalhados sobre análise e gestão de risco. O panfleto do Air Force Systems Command AFSCP 800-45 [AFC88] descreve técnicas de identificação e redução de riscos. Todas as edições do *ACM Software Engineering Notes* têm uma seção denominada "Risks to the Public" (editor, P. G. Neumann). Se você quiser conhecer as mais recentes e melhores histórias de horror do software, essa é a página a ser lida.

Há disponível na Internet uma grande variedade de fontes de informação sobre gestão de risco de software. Uma lista atualizada das referências da Web pode ser encontrada no site **www.mhhe.com/engcs/compsci/pressman/professional/olc/ser.htm**.