



Rafael de Souza Lima Espinha

**Uma Abordagem para a Avaliação de Processos de
Desenvolvimento de Software Baseada em Risco e
Conformidade**

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para
obtenção do título de Mestre pelo Programa de Pós-
Graduação em Informática da PUC-Rio.

Orientadores: Arndt von Staa
Carlos José Pereira de Lucena

Rio de Janeiro, 27 de março de 2007



Rafael de Souza Lima Espinha

Uma Abordagem para a Avaliação de Processos de Desenvolvimento de Software Baseada em Risco e Conformidade

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Informática da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Arndt Von Staa

Orientador

Departamento de Informática - PUC-Rio

Prof. Carlos José Pereira de Lucena

Co-Orientador

Departamento de Informática PUC-Rio

Prof. Clenio Figueiredo Salviano

Divisão de Melhoria de Processo de Software - Centro de Pesquisa

Renato Archer

Profa. Karin Koogan Breitman

Departamento de Informática - PUC-Rio

Prof. Ricardo Choren Noya

Instituto Militar de Engenharia

Prof. José Eugenio Leal

Coordenador Setorial do Centro Técnico Científico - PUC-Rio

Rio de Janeiro, 27 de março de 2007

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

Rafael de Souza Lima Espinha

Graduou-se em Engenharia de Computação pela PUC-Rio em 2004, onde continuou seus estudos no programa de Mestrado em Informática. É pesquisador associado ao Laboratório de Engenharia de Software e consultor da PrimeUp, onde desenvolve projetos na área de processos e qualidade de software.

Ficha Catalográfica

Espinha, Rafael de Souza Lima

Uma abordagem para a avaliação de processos de desenvolvimento de software baseada em risco e conformidade / Rafael de Souza Lima Espinha ; orientadores: Arndt Von Staa, Carlos José Pereira de Lucena. – 2007.

132 f. : il. ; 30 cm

Dissertação (Mestrado em Informática)–Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

Inclui bibliografia

1. Informática – Teses. 2. Processos de desenvolvimento. 3. Avaliação de processos. 4. Normas de qualidade. 5. Análise de risco. 6. Análise de conformidade. 7. Engenharia de software. 8. Qualidade de software. I. Staa, Arndt Von. II. Lucena, Carlos José Pereirs de. III. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. IV. Título.

CDD: 004

Para meus pais, meu irmão e minha namorada.

Agradecimentos

A Deus, por ter me ajudado a trilhar meu caminho.

À minha família, pela ajuda e apoio ao longo deste trabalho e de toda minha vida.

À minha namorada e companheira, Joanna, por sempre acreditar e compartilhar dos meus sonhos e ideais.

Ao meu orientador, Professor Arndt von Staa, pela ajuda e participação no desenvolvimento deste trabalho.

Ao meu co-orientador, Professor Carlos José Pereira de Lucena, pelo apoio a este trabalho.

À CAPES, CNPq e PUC-Rio, pelos auxílios concedidos e, sem os quais este trabalho não poderia ser realizado.

A todos os integrantes da PrimeUp, em especial Gustavo Carvalho e Leandro Daflon, pelas revisões e valiosas contribuições neste trabalho.

Aos meus amigos do LES, pelo companheirismo e amizade ao longo destes quatro anos.

À Módulo Security, por todo apoio durante a customização do Check-up Tool.

Resumo

Espinha, Rafael de Souza Lima; Staa, Arndt von; Lucena, Carlos José Pereira de. **Uma Abordagem para a Avaliação de Processos de Desenvolvimento de Software Baseada em Risco e Conformidade**. Rio de Janeiro, 2007. 132p. Dissertação de Mestrado - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Atualmente, um dos principais requisitos de um projeto de desenvolvimento de software é a entrega de um produto de qualidade que obedeça ao prazo e orçamento estipulados e atenda às necessidades do cliente. Utilizando a premissa de que a qualidade do produto desenvolvido está intimamente relacionada à qualidade dos processos utilizados no seu desenvolvimento, muitas organizações investem em programas de melhoria contínua de processos, onde estes processos são constantemente avaliados e melhorados. Este trabalho propõe uma abordagem para a avaliação de processos baseada em análise do risco e da conformidade em processos de desenvolvimento. Esta abordagem é constituída por um método de avaliação em duas etapas e por uma ferramenta de apoio. Na primeira fase do método, uma avaliação em abrangência é realizada para identificar em que áreas se encontram os maiores problemas nos processos. Na segunda fase, uma avaliação mais elaborada e criteriosa é realizada apenas nas áreas críticas, diminuindo o custo e aumentando a eficiência do investimento em melhoria. A ferramenta utiliza um mecanismo de questionários e *checklists* para verificar o risco e a conformidade dos processos da organização. Estes questionários e *checklists* estão associados a uma base de conhecimento organizada segundo um modelo de maturidade ou norma de qualidade de referência. Ao final de uma avaliação são gerados relatórios, tabelas e gráficos que apóiam a tomada de decisão e orientam a elaboração de um plano de ação para a melhoria dos processos. A abordagem foi utilizada em três experimentos controlados.

Palavras-chave

Processos de Desenvolvimento, Avaliação de Processos, Normas de Qualidade, Análise de Risco, Análise de Conformidade, Engenharia de Software, Qualidade de Software, Melhoria Contínua.

Abstract

Espinha, Rafael de Souza Lima; Staa, Arndt von; Lucena, Carlos José Pereira de.. **A Compliance and Risk-Based Software Development Process Assessment Approach.** Rio de Janeiro, 2007. 132p. Master Dissertation – Computer Science Department, Pontifical Catholic University of Rio de Janeiro.

Nowadays, one of the main requirements of a software development project is the delivery of a quality product that conforms to the expected schedule and budget and satisfies customer needs. Using the hypothesis that the quality of the developed product is closely related to the quality of the processes used in its development, many organizations invest in process improvement programs, where the processes are continuously assessed and improved. In this work we propose an approach for process assessment based on risk and process compliance analysis. This approach is composed of a two-step appraisal method and a supporting tool. In the first step of the method, a quick analysis is executed to identify the most problematic areas. In the second one, a more elaborated analysis is performed only in the critical areas, reducing the costs and increasing the effectiveness of the appraisal. The tool uses a mechanism of surveys and checklists to verify the risk and the compliance of the process of the organization. A knowledge base is organized in accordance to a reference quality norm or maturity model. At the end of an assessment, reports, tables and charts support the decision-taking, and they can be used to guide an improvement program. The approach has been used in three case studies.

Keywords

Development Processes, Process Assessment, Maturity Models, Risk Analysis, Compliance Analysis, Software Engineering, Software Quality, Continuous Improvement.

Sumário

| | |
|---|----|
| 1 Introdução | 14 |
| 1.1. Melhoria Contínua | 15 |
| 1.2. Motivação | 16 |
| 1.3. Guia do Leitor | 18 |
| 2 Análise de Risco | 20 |
| 2.1. Gerência de Risco | 20 |
| 2.2. Análise de Risco em Processos | 22 |
| 3 Método PAM | 24 |
| 3.1. Requisitos do Método | 25 |
| 3.2. Implementação do Método | 27 |
| 3.2.1. Avaliação em Abrangência | 27 |
| 3.2.2. Avaliação em Profundidade | 30 |
| 3.2.3. Elaboração e Implantação de um Plano de Ação | 31 |
| 4 Ferramenta de Análise de Risco em Processos de Software | 33 |
| 4.1. Check-up Tool | 33 |
| 4.1.1. Metodologia de Análise de Risco | 34 |
| 4.1.2. Estrutura da Ferramenta | 36 |
| 4.2. Estrutura dos Checklists | 41 |
| 4.3. Customizações para Análise de Processos de Software | 44 |
| 4.3.1. Desenvolvimento de Checklists | 44 |
| 4.3.2. Identificação dos Checklists | 46 |
| 4.3.3. Customização da Estrutura dos Checklists | 47 |
| 4.3.4. Tabelas e Gráficos | 49 |
| 4.3.5. Relatórios | 56 |
| 4.3.6. Determinação da Severidade dos Controles | 59 |
| 4.3.7. Preenchimento dos Controles | 59 |
| 4.3.8. Identificação dos Objetivos do Negócio | 60 |

| | |
|--|-----|
| 5 Estudo de Caso | 61 |
| 5.1. Elaboração dos Checklists | 61 |
| 5.1.1. Checklist de Abrangência | 61 |
| 5.1.2. Checklists de Profundidade | 64 |
| 5.2. Equipe 1 | 68 |
| 5.2.1. Avaliação em Abrangência | 69 |
| 5.2.2. Avaliação em Profundidade | 73 |
| 5.3. Equipe 2 | 76 |
| 5.3.1. Avaliação em Abrangência | 77 |
| 5.3.2. Avaliação em Profundidade | 82 |
| 5.3.3. Avaliação em Profundidade - CMMI | 87 |
| 5.4. Equipe 3 | 87 |
| 5.4.1. Avaliação em Abrangência | 87 |
| 5.4.2. Avaliação em Profundidade | 91 |
| 6 Trabalhos Relacionados | 96 |
| 6.1. Métodos de Avaliação | 96 |
| 6.1.1. SCAMPI | 96 |
| 6.1.2. MA – MPS | 99 |
| 6.1.3. ISO/IEC – 15504 | 100 |
| 6.1.4. PRIME | 103 |
| 6.2. Ferramentas de Avaliação | 104 |
| 6.2.1. CMM – Quest e Appraisal Wizard | 105 |
| 6.2.2. S:Primer + | 105 |
| 7 Conclusão e Trabalho Futuro | 107 |
| 7.1. Trabalho Futuro | 108 |
| Referências | 110 |
| Apêndice A Tabela de Classificação de Diretivas do MPS.BR para a Elaboração do Checklist de Abrangência | 113 |

| | |
|---|-----|
| Apêndice B Exemplo de Controle – Avaliação em Profundidade da Área de Processo Planejamento de Projeto (CMMI-Dev 1.2) | 121 |
| Apêndice C Checklist de Abrangência baseado no MPS.BR | 122 |
| Apêndice D Lista de Objetivos do Negócio e Objetivos de TI | 126 |

Lista de Figuras

| | |
|--|----|
| Figura 1: ciclo do modelo IDEAL | 15 |
| Figura 2: Método PAM | 27 |
| Figura 3: Método PAM – Processo de avaliação em abrangência | 28 |
| Figura 4: Estrutura da metodologia de análise de riscos da ferramenta Check-up Tool (ref. manual de utilização). | 35 |
| Figura 5: Abordagem para a realização de avaliações da ferramenta Check-up Tool | 37 |
| Figura 6: Definição da Estrutura Organizacional | 37 |
| Figura 7: Mapeamento entre objetivos do negócio e ativos da organização | 39 |
| Figura 8: Seleção de escopo do projeto de avaliação | 40 |
| Figura 9: Preenchimento de um <i>checklists</i> na ferramenta Check-up Tool | 41 |
| Figura 10: Estrutura dos agrupamentos de um <i>checklist</i> | 42 |
| Figura 11: Estrutura da base de conhecimento da ferramenta Check-up Tool | 44 |
| Figura 12: Processo de desenvolvimento de <i>checklists</i> | 45 |
| Figura 13: <i>Checklist</i> com agrupamentos para características específicas e genéricas | 48 |
| Figura 14: Gráfico Relevância x Risco de Agrupamentos | 55 |
| Figura 15: Gráfico de Consolidação dos Resultados em Ativos, Objetivos do Negócio e Objetivos de TI | 56 |
| Figura 16: Risco nas áreas de processo | 71 |
| Figura 17: Equipe 2 – Visão geral dos resultados da avaliação em abrangência | 78 |
| Figura 18: Equipe 2 – Visão geral dos resultados da avaliação em profundidade | 83 |
| Figura 19: Equipe 3: Visão geral dos resultados da avaliação em abrangência | 89 |
| Figura 20: Equipe 3: Visão geral dos resultados da avaliação em profundidade | 92 |

Lista de Tabelas

| | |
|--|----|
| Tabela 1: Classificação dos valores da Probabilidade, Severidade e Relevância | 35 |
| Tabela 2: Interpretação dos valores do índice PSR | 36 |
| Tabela 3: Classificação da relevância dos ativos | 39 |
| Tabela 4: Ameaças para o domínio de processos de software | 48 |
| Tabela 5: 10 Controles com Maior Risco | 50 |
| Tabela 6: 10 C0ntroles com Maior Risco Total | 50 |
| Tabela 7: Risco por Controle | 51 |
| Tabela 8: Risco Total por Controle | 51 |
| Tabela 9: Risco Total por Ativo | 52 |
| Tabela 10: Risco Total por Ativo | 52 |
| Tabela 11: Risco Total por Ameaça | 53 |
| Tabela 12: Risco Total por Checklist | 53 |
| Tabela 13: Situação dos Controles | 53 |
| Tabela 14: formato de apresentação de dados do Relatório Operacional de Risco | 57 |
| Tabela 15: Classificação de severidade das ameaças | 63 |
| Tabela 16: Agrupamentos utilizados no checklist de abrangência | 63 |
| Tabela 17: Agrupamentos adicionados para os <i>checklists</i> de profundidade | 64 |
| Tabela 18: Agrupamentos adicionados para o CMMI | 65 |
| Tabela 19: Resumo dos estudos de caso realizados | 66 |
| Tabela 20: Equipe 1 - Resultado consolidado nos objetivos de negócio | 70 |
| Tabela 21: Equipe 1 – Resultado consolidado por áreas de processo | 72 |
| Tabela 22: Equipe 1 – Análise de conformidade | 73 |
| Tabela 23: Equipe 1 - 10 Controles com Maior Risco Total | 75 |
| Tabela 24: Equipe 2 – Risco total por participantes | 79 |
| Tabela 25: Equipe 2 – Risco total por área de processo para o ativo Gerente | 80 |
| Tabela 26: Equipe 2 – Risco total por área de processo para o ativo Participante 1 | 80 |
| Tabela 27: Equipe 2 – Risco total por área de processo | 81 |

| | |
|--|----|
| Tabela 28: Equipe 2 – Consolidação do risco total por objetivos do negócio | 82 |
| Tabela 29: Equipe 2: Consolidação do risco total por <i>checklist</i> (área de processo) | 84 |
| Tabela 30: Equipe 2: Risco total por agrupamento (atributos genéricos e específicos) para a área de processo de Gerência de Requisitos | 84 |
| Tabela 31: Equipe 2: Risco total por agrupamento (atributos genéricos e específicos) para a área de processo de Gerência do Projeto | 84 |
| Tabela 32: Equipe 2: 10 Controles com Maior Risco Total | 85 |
| Tabela 33: Equipe 3 – Resultados consolidados por perímetro avaliado | 90 |
| Tabela 34: Equipe 3: Resultados consolidados por objetivo do negócio | 90 |
| Tabela 35: Equipe 3 – Resultado consolidado dos agrupamentos, para os objetivos do negócio selecionados | 91 |
| Tabela 36: Equipe 3 - 10 Controles com Maior Risco Total | 93 |