

## 4

### Ferramenta de Análise de Risco em Processos de Software

A segunda parte deste trabalho consistiu na customização de uma ferramenta para apoiar a execução de avaliações que utilizem o método PAM. Após a realização de uma pesquisa de ferramentas disponíveis no mercado, onde as ferramentas Check-up Tool, Appraisal Wizard, CMM – Quest e S:Primer+ apresentadas no Capítulo 6 foram identificadas e estudadas, e de uma análise comparativa entre os benefícios e dificuldades da customização de uma ferramenta já existente e do desenvolvimento de uma nova, chegou-se a conclusão de que a primeira ofereceria maiores vantagens. Esta decisão baseou-se em dois fatores: Esforço necessário para o desenvolvimento/customização (*time to market*) e aceitação no mercado.

Sendo assim, foi selecionada a ferramenta Check-up Tool, desenvolvida pela Módulo Security, que oferece suporte a execução de avaliações de conformidade e risco utilizando uma abordagem baseada nas Normas ISO/IEC TR 13335-1:1996 (ISO/IEC, 1996), ISO/IEC 17799 (ISO/IEC, 2005) e ISO Guide 73:2002 (ISO/IEC, 2002) e possui grande aceitação no mercado em diversos domínios de aplicação.

#### 4.1.

##### Check-up Tool

A ferramenta Check-up Tool foi desenvolvida pela Módulo Security com o intuito de apoiar avaliações de conformidade e risco relativas a segurança da informação. Utilizando como base modelos de maturidade e normas de qualidade e tendo como instrumento principal a utilização de *checklists*, a ferramenta fornece uma base de conhecimento para a verificação da correta implementação das diretivas do modelo ou norma utilizada, além de recomendações de implementação para os casos em que esta não esteja presente na organização avaliada.

Estando no mercado desde março de 2000, a ferramenta foi utilizada em mais de 400 projetos de avaliação e implementação de modelos de maturidade e

normas de qualidade na área de segurança da informação. Ao longo dos últimos anos, foi iniciado um estudo da utilização da ferramenta para outros domínios de aplicação, através da utilizando a estrutura de análise de risco e conformidade e da customização da sua base de conhecimento associada. Esta iniciativa gerou distribuições para as mais diversas áreas, tais como controle de febre aftosa e análise de contratos do ponto de vista jurídico, cuja eficácia foi comprovada na realização de diversos projetos (Módulo, 2007).

#### **4.1.1.**

##### **Metodologia de Análise de Risco**

A metodologia de análise de risco utiliza o conceito básico apresentado no capítulo 3.2, onde a exposição ou nível de risco é calculado através da probabilidade e do impacto da sua ocorrência. Além disto, o conceito de ameaças é explorado por representar problemas que podem se aproveitar de uma fraqueza da organização gerada pela não implementação de alguma diretiva do modelo de maturidade ou norma de qualidade e se manifestar.

O item de verificação dos riscos é o ponto onde os dados são coletados para identificar o nível de exposição a riscos da organização. Uma organização é avaliada segundo os seus ativos organizacionais, representados por seus processos, pessoas, papéis, tecnologia ou ambiente. Os instrumentos de coleta de dados são os controles, que verificam a implementação das diretivas do modelo de maturidade ou norma de qualidade utilizada como referência. Um exemplo de controle pode ser visto no Apêndice B.

A Figura 4 ilustra a estrutura da metodologia utilizada pela ferramenta Check-up Tool.

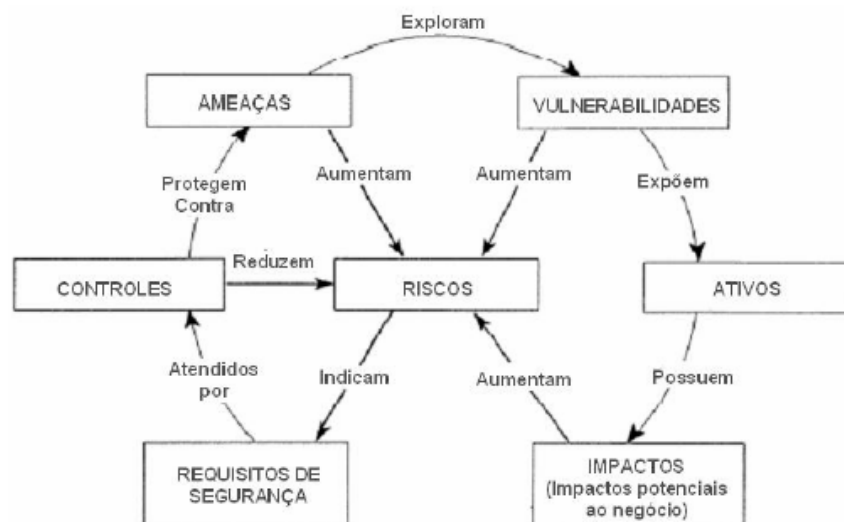


Figura 4: Estrutura da metodologia de análise de riscos da ferramenta Check-up Tool (ref. manual de utilização).

Para tornar o cálculo do nível de risco mais eficiente, o conceito de impacto foi fragmentado em duas variáveis: Severidade e Relevância. A primeira indica o impacto no ativo e na organização da concretização das ameaças associadas ao risco. A segunda indica o grau de importância do ativo para o negócio da empresa, considerando os componentes de negócio que ele apóia, e calibra o impacto do risco (ativos menos relevantes possuem um alcance de impacto menor e, consequentemente, contribuem menos com o nível de risco).

Sendo assim, foi criado o índice PSR, que representa quantitativamente o nível de risco calculado através da Probabilidade da ocorrência do risco, da Severidade desta ocorrência e da relevância do ativo comprometido para a organização. Durante a configuração da avaliação, um valor de 1 a 5 é determinado para a Relevância de cada ativo e para a Severidade e Probabilidade de cada controle de verificação, de acordo com a classificação indicada na Tabela 1. O valor final do nível de risco (índice PSR), cuja interpretação encontra-se na Tabela 2, é a multiplicação dos valores das três variáveis.

Tabela 1: Classificação dos valores da Probabilidade, Severidade e Relevância

PSR				
	PROBABILIDADE A ocorrência da vulnerabilidade ser explorada pelas ameaças:	SEVERIDADE A consequência da vulnerabilidade ser explorada pelas ameaças:	RELEVÂNCIA O comprometimento da segurança do ativo:	
5	É quase certa (≥ 95%)	Afetar <sup>á</sup> extremamente a segurança	Pode afetar toda a empresa e os prejuízos serão extremamente altos	MUITO ALTA
4	É muito provável (65% ≤ P < 95%)	Afetar <sup>á</sup> muito gravemente a segurança	Pode afetar um ou mais negócios da empresa e os prejuízos serão muito altos	ALTA
3	É provável (35% ≤ P < 65%)	Afetar <sup>á</sup> gravemente a segurança	Pode afetar uma parte do negócio da empresa e os prejuízos serão razoáveis	MÉDIA
2	É improvável (5% ≤ P < 35%)	Afetar <sup>á</sup> pouco a segurança	Pode afetar uma parte pequena e localizada do negócio da empresa e os prejuízos serão baixos	BAIXA
1	É muito improvável (< 5%)	Quase não afetar <sup>á</sup> a segurança	Pode afetar uma parte muito pequena e localizada do negócio da empresa e os prejuízos serão desprezíveis	MUITO BAIXA

Tabela 2: Interpretação dos valores do índice PSR

Nível de Risco	Valores Possíveis PSR*
Muito Baixo	1,2,3,4,5,6
Baixo	8,9,10,12,15,16
Médio	18,20,24,25,27,30
Alto	32,36,40,45,48,50
Muito Alto	60,64,75,80,100,125

A partir do cálculo do índice PSR de cada controle, pode-se gerar um vasto número de interpretações, através do agrupamento de elementos e da determinação de índices relativos (índice de segurança =

$$\frac{PSR_{\text{controles implementados}}(\text{elemento})}{PSR(\text{Total})}; \text{ índice de risco} = 1 - \text{índice de segurança}; \text{ participação}$$

do elemento no risco total, etc.), que irão guiar o processo de tomada de decisão.

#### 4.1.2. Estrutura da Ferramenta

A estrutura da ferramenta define três etapas para a realização da avaliação. A primeira etapa consiste na definição da estrutura organizacional que será alvo de algum projeto de avaliação com a utilização da ferramenta. A segunda representa a configuração de um projeto de avaliação, onde um subconjunto do escopo organizacional e do modelo de maturidade ou norma de qualidade é

selecionado como o contexto que será avaliado em uma iteração do ciclo de melhoria. A terceira etapa consiste na execução e acompanhamento da avaliação, através da distribuição e preenchimento dos *checklists*. A Figura 5 abaixo ilustra esta abordagem.

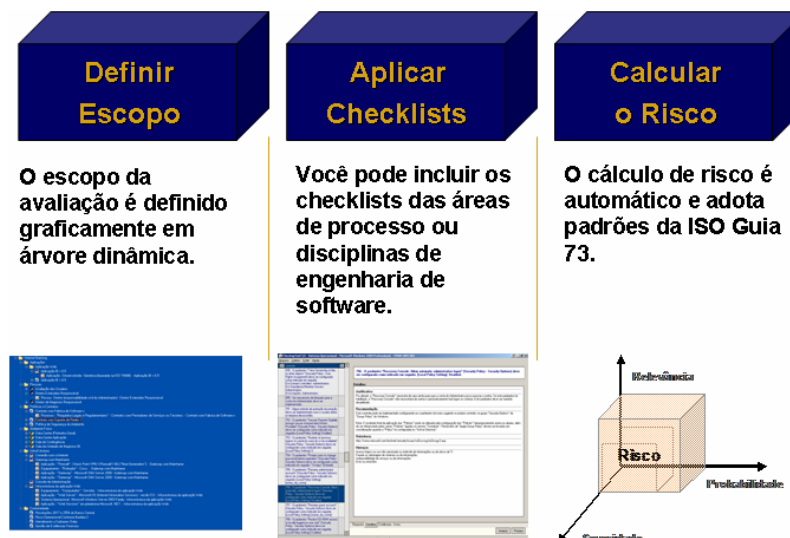


Figura 5: Abordagem para a realização de avaliações da ferramenta Check-up Tool

As etapas serão apresentadas com mais detalhes nas seções abaixo.

#### 4.1.2.1.

##### Definição da Estrutura Organizacional

Nesta etapa, a estrutura organizacional é mapeada, identificando as suas unidades e ativos. A Figura 6 ilustra esta estrutura.

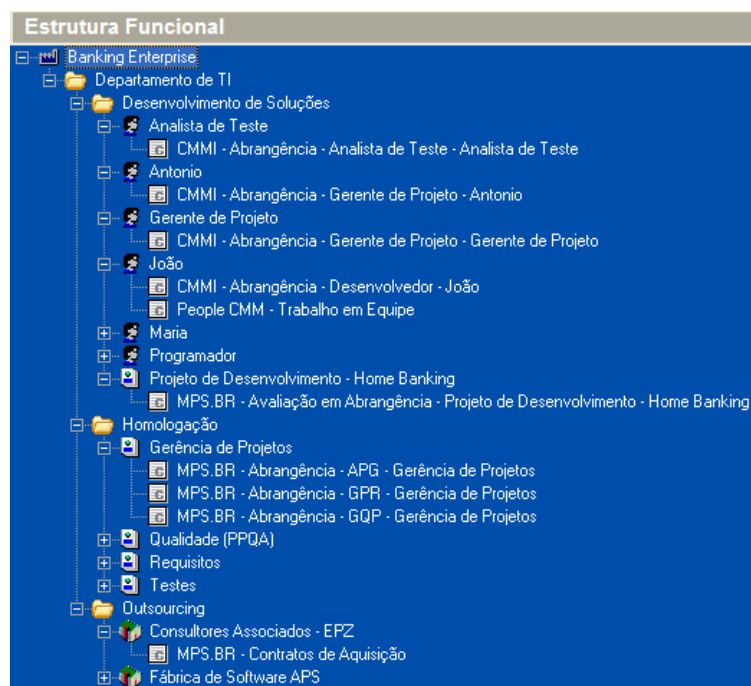


Figura 6: Definição da Estrutura Organizacional

Uma unidade organizacional identifica os departamentos, áreas, projetos ou equipes da organização ou de um projeto, definindo os perímetros da organização. Cada unidade possui um conjunto de ativos que representam os seus processos, pessoas, papéis e fornecedores, ou seja, os ativos identificam os principais recursos que participam no desenvolvimento do produto da organização e que, consequentemente, representam os pontos de verificação de riscos e conformidade do processo produtivo.

Para cada ativo são adicionados componentes que representam quais diretivas ou conjunto de diretivas podem ser verificados através da sua análise. Um ativo pode fornecer dados para a verificação de várias diretivas de diversos modelos de maturidade e norma de qualidade, como pode ser visto no exemplo da Figura 6, onde o ativo João pode fornecer dados relativos ao CMMI e ao People CMM (Curtis, Hefley, Miller, 2006). Cada componente é associado a um *checklist*, que representa o instrumento pelo qual os dados serão coletados no ativo.

Cada organização possui um conjunto de objetivos do negócio associados, sendo que estes podem ser definidos em dois níveis. Cada objetivo do negócio de maior nível deve ser mapeado em objetivos do negócio de menor nível, indicando como este pode ser atingido. Os objetivos do negócio de menor nível de abstração devem ser mapeados nos ativos da organização, indicando quais elementos da estrutura organizacional contribuem para quais objetivos do negócio. A Figura 7 ilustra este mapeamento.

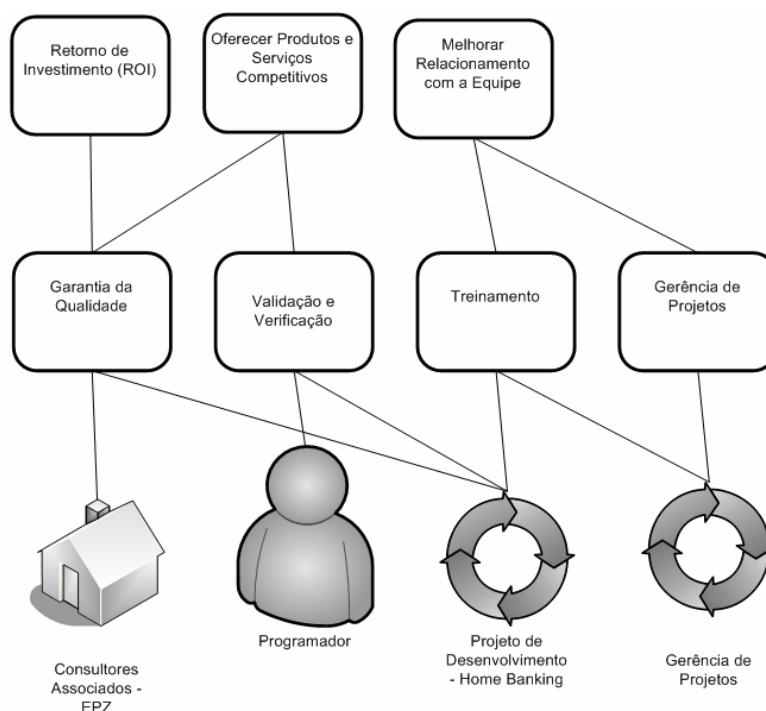


Figura 7: Mapeamento entre objetivos do negócio e ativos da organização

Tendo os objetivos do negócio identificados e organizados em níveis hierárquicos, deve-se identificar a relevância de cada objetivo de nível mais alto para a organização e mapear esta classificação até o nível dos ativos. Esta classificação da relevância dos objetivos do negócio e dos ativos deve gerar um índice de 1 a 5, de acordo com a Tabela 3. Este índice será utilizado no cálculo do índice de risco nas avaliações realizadas.

Tabela 3: Classificação da relevância dos ativos

Nível	Relevância	Classificação
5	Pode afetar toda a empresa e os prejuízos serão extremamente altos.	Muito Alta
4	Pode afetar um ou mais negócios da empresa e os prejuízos serão altos.	Alta
3	Pode afetar uma parte do negócio da empresa e os prejuízos serão razoáveis	Média
2	Pode afetar uma parte pequena e localizada do negócio da empresa e os prejuízos serão baixos.	Baixa
1	Pode afetar uma parte pequena e localizada do negócio da empresa e os prejuízos serão desprezíveis.	Muito Baixa

#### 4.1.2.2. Configuração do Projeto de Avaliação

A segunda etapa de uma avaliação representa o planejamento da execução da avaliação. Nela um projeto de avaliação é cadastrado e identificado, através do

preenchimento do seu nome, descrição e dos avaliadores (líder e substituto). Em seguida um subconjunto da estrutura organizacional é selecionado, definindo-se o escopo da avaliação. Os componentes contidos neste conjunto irão determinar os *checklists* de verificação que serão utilizados durante a avaliação. A Figura 8 ilustra a seleção do escopo de avaliação na ferramenta com um exemplo onde apenas o perímetro “Homologação” foi selecionado e os componentes dos ativos “Testes” e “Gerência de Projetos” foram retirados.

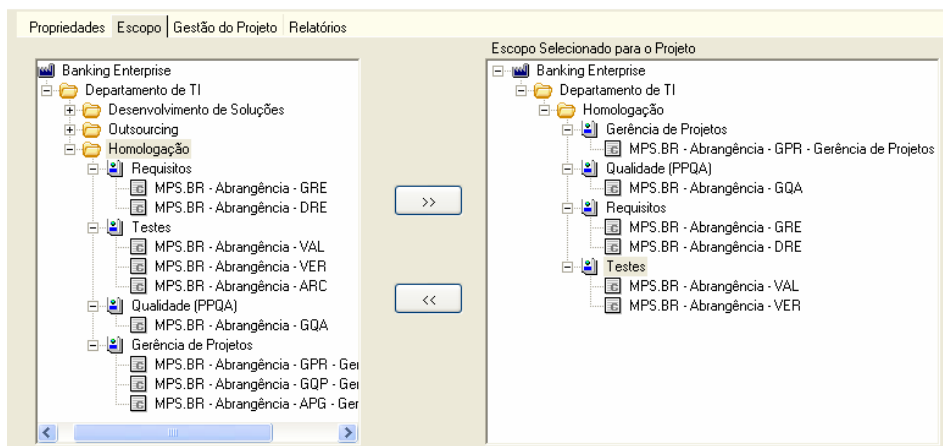


Figura 8: Seleção de escopo do projeto de avaliação

Ao contrário da etapa de Definição da Estrutura Funcional, que é executada apenas uma vez para cada organização, esta etapa é executada toda vez que uma avaliação é realizada. Dessa forma mantém-se o histórico das avaliações, o que permite o acompanhamento da evolução da qualidade e do controle de riscos do processo e fornece dados para a identificação de falhas nos planos de ação utilizados no programa de melhoria contínua.

#### 4.1.2.3. Execução e Acompanhamento da Avaliação

Nesta etapa a avaliação é executada, através do preenchimento dos *checklists* associados aos componentes do escopo do projeto de avaliação. O preenchimento pode ser feito diretamente pelo avaliador, através de um módulo de resposta *offline* ou por questionários distribuídos via e-mail.

Cada *checklist* possui um conjunto de controles, que representam um ponto atômico de verificação de uma diretiva ou parte de uma diretiva do modelo ou norma de referência (a estrutura dos *checklists* será apresentada com mais detalhes na próxima seção), sendo que cada controle possui uma probabilidade e severidade associada. O valor destas variáveis é definido para um ambiente



genérico durante a elaboração do *checklist* e pode ser customizado pelo avaliador, de acordo com a característica da organização, do projeto ou do ativo.

Durante o preenchimento dos *checklists*, seus controles são respondidos, associando-se a eles um dos seguintes valores: Implementado, Não Implementado, Não Aplicável e Não Respondido. Para cada controle podem ser cadastrados comentários e evidências que corroborem ou justifiquem o valor associado. A Figura 9 ilustra o preenchimento dos *checklists*.

The screenshot displays the 'Check-up Tool' interface. On the left, a table lists several controls under the 'Agrupamento : Documentation' group. The first control, '10000012 - GRE 1. Uma comunicação contínua com os fornecedores de requisitos deve ser estabelecida.', is marked with a green checkmark. The right pane shows the details for this control. It includes a 'Situação' (Status) section with radio buttons for 'Implementado' (selected), 'Não Implementado', 'Não Aplicável', and 'Não Respondido'. Below this are dropdown menus for 'Probabilidade' (set to 'Baixa (>5% e <=35%)') and 'Severidade' (set to 'Média'). There is also a 'Relevância do Ativo' (Asset Relevance) section with a radio button for 'Muito Alta'. A large text area for 'Comentário' (Comment) contains the text: 'Não existe uma política de identificação de fontes de requisitos e estabelecimento de comunicação. Apenas o responsável pelos requisitos entra em contato com o cliente, que é representado pelo contratante do projeto ou por alguém indicado por ele.' At the bottom, there are tabs for 'Resposta', 'Detalhes', 'Evidências', and 'Aviso'.

Figura 9: Preenchimento de um *checklists* na ferramenta Check-up Tool

Quando um *checklist* está totalmente preenchido, ele deve ser fechado. Quando todos os *checklists* são fechados, a etapa de execução da avaliação é finalizada. A partir daí um conjunto de relatórios, tabelas e gráficos pode ser gerado e utilizado, diretamente ou após uma customização, no apoio a tomada de decisão. Diversos níveis de relatórios, gráficos e tabelas podem ser gerados pela ferramenta, permitindo uma análise tanto no nível dos controles e dos ativos quanto uma análise dos resultados consolidados nos perímetros, ameaças e nos objetivos do negócio da organização. Uma série de filtros também está disponível para geração dos relatórios, tornando possível selecionar os perímetros, tipos de ativo, objetivos do negócio, *checklists* e outros parâmetros.

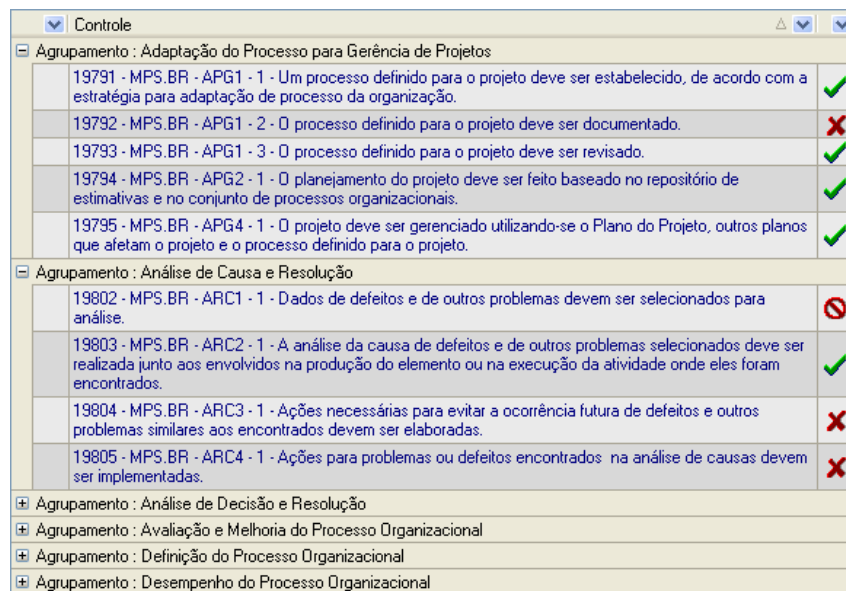
Durante o período de execução é possível acompanhar o preenchimento dos *checklists* e gerar relatórios preliminares.

#### 4.2. Estrutura dos Checklists

Como pode ser notado nas seções anteriores deste capítulo, o principal elemento da ferramenta Check-up Tool são os *checklists*. Estes representam os

pontos de extensão da ferramenta, permitindo que bases de conhecimento dos mais diversos domínios de aplicação possam utilizar a infra-estrutura de análise de risco e conformidade.

Um *checklist* representa uma característica do domínio de avaliação (ex. PAs do CMMI ou processos do MPS.BR) que será verificado em um ativo da organização, durante um projeto de avaliação. Cada *checklist* é composto de itens atômicos de verificação, denominados controles, que representam uma diretiva ou um pedaço de uma diretiva do modelo ou norma de referência, sendo que estes controles podem ser categorizados em agrupamentos compartilhados por todos os *checklists* de um mesmo domínio. A Figura 10 ilustra esta estrutura com um *checklist* baseado no modelo MPS.BR, onde os agrupamentos representam os processos.



Controle		Status
<b>Agrupamento : Adaptação do Processo para Gerência de Projetos</b>		
19791 - MPS.BR - APG1 - 1 - Um processo definido para o projeto deve ser estabelecido, de acordo com a estratégia para adaptação de processo da organização.		✓
19792 - MPS.BR - APG1 - 2 - O processo definido para o projeto deve ser documentado.		✗
19793 - MPS.BR - APG1 - 3 - O processo definido para o projeto deve ser revisado.		✓
19794 - MPS.BR - APG2 - 1 - O planejamento do projeto deve ser feito baseado no repositório de estimativas e no conjunto de processos organizacionais.		✓
19795 - MPS.BR - APG4 - 1 - O projeto deve ser gerenciado utilizando-se o Plano do Projeto, outros planos que afetam o projeto e o processo definido para o projeto.		✓
<b>Agrupamento : Análise de Causa e Resolução</b>		
19802 - MPS.BR - ARC1 - 1 - Dados de defeitos e de outros problemas devem ser selecionados para análise.		✗
19803 - MPS.BR - ARC2 - 1 - A análise da causa de defeitos e de outros problemas selecionados deve ser realizada junto aos envolvidos na produção do elemento ou na execução da atividade onde eles foram encontrados.		✓
19804 - MPS.BR - ARC3 - 1 - Ações necessárias para evitar a ocorrência futura de defeitos e outros problemas similares aos encontrados devem ser elaboradas.		✗
19805 - MPS.BR - ARC4 - 1 - Ações para problemas ou defeitos encontrados na análise de causas devem ser implementadas.		✗
<b>Agrupamento : Análise de Decisão e Resolução</b>		
<b>Agrupamento : Avaliação e Melhoria do Processo Organizacional</b>		
<b>Agrupamento : Definição do Processo Organizacional</b>		
<b>Agrupamento : Desempenho do Processo Organizacional</b>		

Figura 10: Estrutura dos agrupamentos de um *checklist*

Cada controle possui uma estrutura com os seguintes elementos:

- **Nome do Controle:** Indica o que deve ser verificado no ativo, perímetro ou na organização para que o controle possa ser preenchido. Representa uma característica que deve estar presente para que o controle seja considerado implementado.
- **Justificativa:** Define termos e conceitos necessários para o entendimento do controle e fornece uma justificativa que explique porque aquele controle deve ser implementado. Neste elemento são apresentadas as vantagens que se obtém com a implementação do controle e as consequências da sua não implementação.

- **Ameaças:** Indica quais ameaças podem se aproveitar da não implementação do controle para se manifestar e causar danos ao negócio da organização.
- **Recomendação:** Este elemento fornece dados para a elaboração de um plano de ação após a realização da avaliação, através de uma sugestão de como o controle pode ser implementado para diminuir a exposição da organização aos riscos e atingir a conformidade desejada com o modelo ou norma de referência.
- **Referências:** Indica referências bibliográficas para que mais informações acerca do controle e da sua implementação possam ser obtidas.
- **Probabilidade:** Representa a probabilidade de uma ameaça se manifestar caso o controle não esteja implementado na organização. Este elemento representa um número de 1 a 5, cujo significado é descrito na Tabela 1.
- **Severidade:** Indica o grau do impacto negativo na organização, caso uma ou mais ameaças se manifestem. Este elemento representa um número de 1 a 5, cujo significado é descrito na Tabela 1.
- **Agrupamento:** Indica a qual agrupamento o controle pertence.

Um exemplo de controle pode ser visto no Apêndice B.

Cada *checklist* pode ter um questionário associado a ele. Este questionário representa uma interpretação dos controles para um público com menor conhecimento do modelo ou norma de referência, definindo uma interface de acesso aos controles e uma lógica de mapeamento entre perguntas e controles, que define como o *checklists* será preenchido com os dados coletados por este meio.

A Figura 11 abaixo utiliza a linguagem UML (OMG, 2007) para representar a estrutura de uma base de conhecimento.

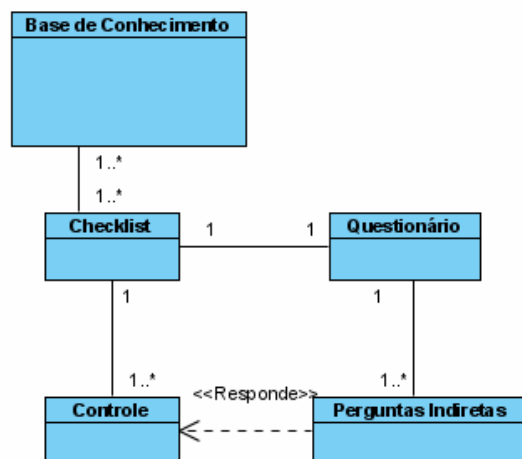


Figura 11: Estrutura da base de conhecimento da ferramenta Check-up Tool

#### 4.3.

#### Customizações para Análise de Processos de Software

Nesta seção serão apresentadas as customizações realizadas na ferramenta Check-up Tool para o domínio de processos de desenvolvimento de software e que constitui uma das contribuições deste trabalho, no que se refere à ferramenta de suporte à avaliação.

Como o objetivo deste trabalho foi o de aproveitar a estrutura da ferramenta, as customizações se concentraram nos seus pontos de extensão, representada pelos *checklists*, tabelas, gráficos e relatórios. Com o intuito de auxiliar a criação de bases de conhecimento para diversos modelos e normas de referência e facilitar a utilização da ferramenta no domínio de processos de desenvolvimento, também foram desenvolvidas abordagens para auxiliar o desenvolvimento e o preenchimento dos *checklists* e uma identificação padrão de objetivos do negócio. Ao longo deste trabalho não foram realizadas alterações na estrutura da ferramenta.

##### 4.3.1.

##### Desenvolvimento de Checklists

Visando padronizar e orientar o desenvolvimento de *checklists* que irão compor uma base de conhecimento, foi definido o processo apresentado abaixo.

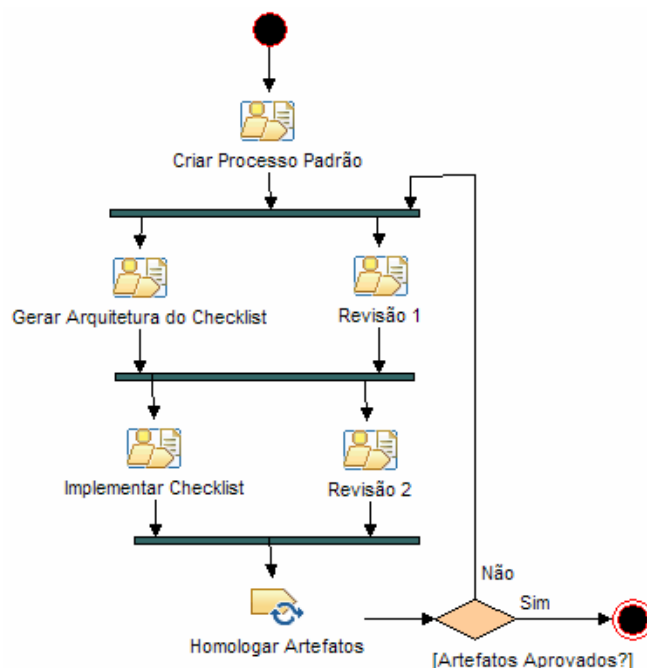


Figura 12: Processo de desenvolvimento de *checklists*

A primeira atividade consiste na criação de um processo padrão para a área de processo ou grupo de áreas de processo, que será utilizado como base para a elaboração das recomendações de implementação de controles. Esta atividade possui tarefas de elaboração e revisão de conteúdo e aderência ao modelo ou norma de qualidade utilizada como referência. Em seguida, atividades de geração de arquitetura e revisão dos artefatos gerados são executadas iterativa e concorrentemente, até que um produto de qualidade assegurada seja desenvolvido. A arquitetura do *checklist* consiste da identificação dos controles que serão desenvolvidos e dos questionários que serão utilizados como coletores automáticos de dados.

Tendo um conjunto revisado dos controles que devem ser implementados e um questionário que interpreta e responde estes controles do *checklist* através de uma lógica bem definida para as suas perguntas, inicia-se uma nova etapa iterativa e concorrente de implementação e revisão dos controles, onde o conteúdo dos controles identificados é elaborado e o questionário desenvolvido é refinado.

Finalmente, quando um *checklist* e um questionário completo para uma área de processo é finalizado, realiza-se uma atividade de homologação, onde um controle de qualidade irá verificar se o produto desenvolvido atende aos padrões e se este pode entrar em produção. Quando o processo é finalizado, o produto

homologado é cadastrado na ferramenta através de um editor de *checklists*, ficando pronto para a utilização em avaliações.

#### 4.3.2.

#### Identificação dos Checklists

O primeiro passo na customização do Check-up Tool para o domínio de processos de desenvolvimento foi a identificação dos *checklists* que seriam utilizados para a realização das avaliações. Como os *checklists* são associados aos ativos da organização, através dos componentes, esta atividade foi realizada utilizando como parâmetro os tipos de ativos.

A ferramenta define quatro tipos de ativo para a realização das avaliações: “Processo”, “Pessoa”, “Ambiente” e “Tecnologia”. Para o domínio de processos de desenvolvimento, definiu-se que cada ativo funcionaria como uma dimensão de coleta de dados sobre os processos da organização ou do projeto ao qual ele pertence. Sendo assim, chegou-se a seguinte taxonomia para os ativos:

- **Processos** representam os processos, áreas de processo ou disciplinas da organização. Cada *checklists* associado a este tipo de ativo possui o escopo de uma área de processo do modelo de maturidade ou norma de qualidade. A utilização de ativos do tipo Processo define uma dimensão da avaliação onde os processos são o principal fator para o alcance dos objetivos da organização e, consequentemente, a principal fonte de evidências da implementação do modelo ou norma de referência.
- **Pessoa** representam os atores da organização. Os *checklists* associados a este tipo de ativo verificam as diretivas da norma relativas a um papel da organização (desenvolvedor, gerente, analista de requisitos, etc.) que é assumido pela pessoa que é referenciada pelo ativo. A utilização de ativos do tipo Pessoa define uma dimensão da avaliação onde as pessoas e os papéis que elas executam são o principal fator para o alcance dos objetivos da organização e, consequentemente, a principal fonte de evidências da implementação do modelo ou norma de referência.
- **Ambiente** representam o ambiente organizacional, caracterizado pelas acomodações, aspectos inter-pessoais, política motivacional e

outros fatores que afetam indiretamente a execução dos processos. Os *checklists* associados a este tipo de ativo verificam as características do ambiente da organização ou de um perímetro específico e como ele contribui ou não com o alcance dos objetivos da organização.

- **Tecnologia** representa a estrutura tecnológica da organização, definida por suas máquinas e ferramentas. Os *checklists* associados a este tipo de ativo verificam características da infra-estrutura tecnológica referenciada pelo ativo, como segurança em servidores, funcionalidades de ferramentas, entre outros.

#### 4.3.3. Customização da Estrutura dos Checklists

Como segundo passo da customização, a estrutura para a geração de *checklists* foi elaborada. Esta atividade contou com a definição dos agrupamentos, ameaças e do escopo dos controles.

Como o objetivo da customização foi obter resultados mapeados nas áreas de processo do modelo ou norma de qualidade de referência, independente de quais ativos foram utilizados para coletar os dados, foi definido que os agrupamentos utilizados seriam as áreas de processo.

Uma área de processo possui características específicas, que determinam a sua implementação, e características comuns a todas as áreas, que determinam a sua capacidade. Para facilitar a utilização de modelos de maturidade que utilizam o conceito de capacidade de processos foi definido também que, para cada área de processo, deve existir um agrupamento para as características específicas e um para as características de cada nível de capacidade.

A Figura 13 ilustra este conceito para o MPS.BR, onde, para a área de processo (ou processo, que é a nomenclatura utilizada pelo modelo) de Gerência de Requisitos, temos o agrupamento “Gerencia de requisitos”, referente às características específicas, e os agrupamentos “GRE - AP1.1 - O Processo é Executado”, “GRE - AP2.1 - O Processo é Gerenciado”, “GRE - AP2.2 - Os Produtos de Trabalho do Processo São Gerenciados”, “GRE - AP3.1 - O Processo é Definido” e “GRE - AP3.2 - O Processo Está Implementado”, referente às características comuns.

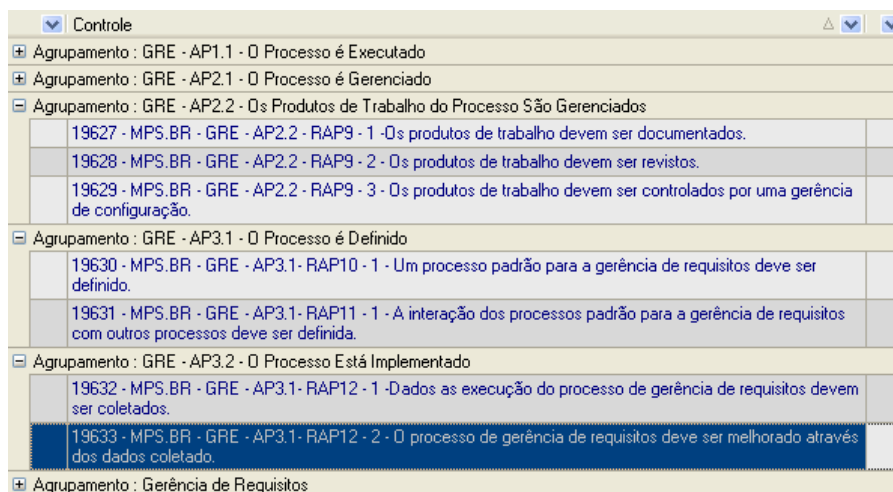


Figura 13: *Checklist* com agrupamentos para características específicas e genéricas

Com a estrutura de agrupamentos definida, os resultados das análises de risco e conformidade podem ser consolidados pelos agrupamentos, resultando em relatórios que indicam risco e conformidade de cada área de processo e que deixam transparente quais tipos de ativo foram utilizados.

Para o escopo dos controles, foi definida a utilização do item de menor granularidade do modelo ou norma de referência. Como em muitos modelos e normas o item de menor granularidade possui mais de um item de verificação em seu escopo, foi definida também a realização de uma análise da atomicidade. Esta análise tem como objetivo quebrar o item em elementos de verificação atômicos, evitando situações de falha no preenchimento do controle (se existem dois ou mais pontos de verificação em um controle, como respondê-lo no caso de algumas estarem implementadas e outras não?).

Finalmente, para uniformizar as análises de risco e conformidade em processos de desenvolvimento realizados com a utilização da ferramenta, foi elaborada a lista de ameaças apresentada na tabela 4 abaixo.

Tabela 4: Ameaças para o domínio de processos de software

Ameaça	Descrição
Acesso indevido aos dados do projeto	Dados do projeto são acessados por pessoas não autorizadas.
Alocação de recursos inadequada	Distribuição incorreta de recursos alocados para o projeto, prejudicando o andamento das atividades da organização e dos projetos. Em alguns casos pode gerar consumo exagerado.
Baixa manutenibilidade	Causa dificuldades para a equipe de desenvolvimento dar suporte ou modificar a aplicação. Compromete o crescimento ou expansão do sistema.
Baixa qualidade	Baixa qualidade associada aos produtos.
Complexidade e dificuldade na resolução de problemas	Dificuldade para solucionar os problemas encontrados na organização, no projeto ou nos produtos desenvolvidos.
Conflitos entre os participantes	Conflitos entre os participantes da organização ou do projeto.
Consumo desnecessário de	Utilização de recursos em atividades e insumos que não agregam valor à



recursos do projeto	organização, aos seus projetos ou aos produtos desenvolvidos.
Definição indevida de prioridades	Identificação incorreta de necessidades, fazendo com que componentes prioritários sejam desenvolvidos tardiamente e que tarefas sejam acompanhadas de forma incorreta (atividades mais relevantes com menos controle do que atividades menos relevantes).
Descumprimento de orçamento	O montante financeiro previsto para a conclusão do projeto ou entrega do produto tende a ser ultrapassado.
Descumprimento de prazo	O tempo previsto para a conclusão do projeto ou entrega do produto tende a ser desobedecido.
Desestabilização do projeto	Atividades e tarefas do projeto não são executadas conforme o planejado. Este cenário pode não atingir os resultados esperados.
Dificuldades de integração do produto.	Dificuldades na integração dos componentes do produto.
Falha de software	Código ineficaz, fora de especificação, incompatível com outros módulos de software ou de hardware, ou falhas provocadas por parâmetros configurados indevidamente. Este cenário pode provocar perda da integridade de dados, falhas de processamento, perda de sincronismo, erros de transmissão ou outras falhas na comunicação de dados ou voz, paralisação de sistemas, etc.
Implementação do produto não atende aos projetos do produto.	Inconsistência entre o que foi projetado e o que foi desenvolvido pelo projeto.
Ineficiência na implementação ou controle de solicitações de mudança	Implementação das solicitações de mudança nos requisitos do sistema em desenvolvimento ocorre de forma desorganizada. Este cenário pode gerar resultados imprevisíveis.
Insatisfação do cliente	Produto não atende às expectativas e necessidades do cliente.
Limitações técnicas	Barreiras técnicas no desenvolvimento do sistema que limitam algumas das suas funcionalidades ou até mesmo tornando impossível a realização de sua definição primária.
Não percepção de situações de risco presentes.	Falta de dados que indicam riscos eminentes ao projeto ou à organização.
Perda de controle sobre os itens de configuração modificados	Alterações nos itens de configuração (ambiente de desenvolvimento, versões de artefatos, baselines) acontecem de forma desestruturada. Este cenário pode resultar em inconsistências e conflitos entre versões e alterações realizadas.
Problemas de comunicação entre os interessados	Comunicação ineficiente entre os interessados no projeto, gerando inconsistências, consumindo recursos dos projetos e dificultando o trabalho colaborativo.
Problemas no acompanhamento do projeto	Dificuldades no acompanhamento da execução das atividades e tarefas do projeto. Este cenário pode gerar dados inconsistentes, dificultando a tomada de medidas corretivas.
Processo com baixa eficiência	Problemas técnicos na execução do processo consomem mais recursos para a realização das tarefas e o desenvolvimento do produto.
Queda de performance do produto	Excesso de utilização de recursos de comunicação ou processamento, ou sobrecarga de tráfego. Este cenário pode provocar queda de performance, perda de produtividade, etc.
Requisitos incompletos, inconsistentes, inválidos, incorretos ou não verificáveis	Conjunto de requisitos com falhas que impedem a correta implementação. Estas falhas representam riscos à implementação de um sistema. Ou ainda o sistema gerado pode não atender às necessidades e expectativa do cliente.
Re-trabalho inútil	Despender tempo em atividades que serão refeitas ou executar o mesmo trabalho mais de uma vez, indicando um ponto de desperdício de recursos.

#### 4.3.4. Tabelas e Gráficos

Utilizando as customizações na estrutura dos *checklists* descritos acima, foi identificado um conjunto de tabelas e gráficos para serem gerados de forma automática pela ferramenta. A identificação utilizou as tabelas e gráficos já existentes como ponto de partida, interpretando e adaptando os termos para o

domínio de processos de desenvolvimento, e sugeriu novas formas de apresentação de dados para cobrir alguns pontos em aberto.

A seguir são apresentadas as representações identificadas.

#### 4.3.4.1.

#### Tabelas

##### 4.3.4.1.1.

#### 10 Controles com Maior Risco

Indica as tuplas <Controle, Ativo> com maior risco associado, fornecendo dados para que ações imediatas de redução de risco possam ser tomadas no nível dos ativos.

Tabela 5: 10 Controles com Maior Risco

Nome Controle	Ativo	Checklist	PSR Máximo	Recomendação
Nome do controle não implementado, que oferece risco ao ativo e à organização.	Nome do ativo atingido.	Nome do checklist ao qual pertence o controle.	Índice de risco associado ao controle (1 - 125).	Recomendação de implementação do controle.

##### 4.3.4.1.2.

#### 10 Controles com Maior Risco Total

Indica os controles cuja soma do PSR das suas instâncias (tupla <Controle, Ativo>) é maior, fornecendo uma visão consolidada no nível da organização ou do escopo da avaliação dos controles cuja implementação é prioritária. Assim como a tabela “10 Controles com Maior Risco”, esta tabela fornece dados para que ações imediatas de redução de risco possam ser tomadas no nível dos ativos, destacando-se os resultados do índice de PSR e da participação do risco do controle nos riscos totais (risco relativo).

Tabela 6: 10 COntroles com Maior Risco Total

Controle	Checklist	Agrupamento	PSR	% do PSR Total	Recomendação
Nome do controle não implementado, que oferece risco ao ativo e à organização.	Nome do checklist ao qual pertence o controle.	Nome do agrupamento ao qual pertence o controle.	Somatório do índice de risco associado ao controle.	% do PSR total da análise de risco que pertence ao controle (risco relativo).	Recomendação de implementação do controle.

##### 4.3.4.1.3.

#### Risco por Controle

Indica o PSR de cada instância de controle (tupla <Controle, Ativo>) organizada pelo agrupamento e pelo índice PSR dos controles. Esta tabela fornece

uma visão completa dos resultados da avaliação e permite visualizar o estado de cada área de processo (quanto maior o número de controles não implementados e quanto maior o índice de PSR associado a eles, mais comprometida está a área de processo).

Tabela 7: Risco por Controle

Controle	Ativo	PSR	Ameaças	Recomendação
- Agrupamento :				
Nome do controle não implementado, que oferece risco ao ativo e à organização.	Nome do ativo atingido.	Índice de risco associado ao controle (1 - 125).	Ameaças associadas a não implementação do controle.	Recomendação de implementação do controle.
Agrupamento :				

#### 4.3.4.1.4.

##### Risco Total por Controle

Indica o PSR consolidado de cada controle analisado, fornecendo uma visão completa da avaliação em um nível mais alto da apresentada na tabela “Risco por Controle”. Esta tabela também é organizada pelo agrupamento e pelo índice PSR dos controles.

Tabela 8: Risco Total por Controle

Controle	PSR	%PSR	Índice de Conformidade	Índice de Segurança
- Agrupamento :				
Nome do controle não implementado, que oferece risco ao ativo e à organização.	Somatório do índice de risco associado ao controle.	% do PSR total da análise de risco que pertence ao controle (risco relativo).	(Número de Controles Implementados)x100/(Número Total de Controles).	(PSR do Controle)x100/(PSR Máximo do Controle).

#### 4.3.4.1.5.

##### Risco Total por Ativo

Indica o resultado da análise agrupado por ativo, permitindo a visualização do estado atual de cada ativo avaliado (índice de PSR e participação no risco total) e a implementação de ações pontuais baseadas nos índices de risco e conformidade de cada *checklist* (diminuição de riscos e/ou aumento da conformidade).

Tabela 9: Risco Total por Ativo

Checklist	PSR (checklist)	%PSR	Índice de Conformidade (checklist)	Índice de Segurança (checklist)
- Ativo :				
Nome do checklist analisado.	Índice de risco associado ao checklist (somatório do PSR dos controles).	% do PSR total da análise de risco que pertence ao checklist (risco relativo).	(Número de Controles Implementados)x100/(Número Total de Controles).	(PSR do Ativo)x100/(PSR Máximo do Ativo).

#### 4.3.4.1.6.

#### Risco Total por Agrupamento

Indica o resultado consolidado da análise para cada agrupamento (conformidade, nível de capacidade e risco de cada área de processo). Esta tabela fornece uma visão mais alta dos resultados, auxiliando o direcionamento de esforços na melhoria dos processos (para diminuir riscos, abordam-se as áreas de processo com maior índice risco ou que contribuem mais com o risco total - %PSR; para atingir um nível de capacidade e/ou maturidade desejado, abordam-se as áreas de processo com menor conformidade e que fazem parte do escopo do nível desejado)

Tabela 10: Risco Total por Ativo

Agrupamento	PSR	Índice de Conformidade	Índice de Segurança	%PSR
Nome do Agrupamento.	Índice de risco associado ao agrupamento (somatório do PSR dos controles).	(Número de Controles Implementados)x100/(Número Total de Controles).	(PSR do Agrupamento)x100/(PSR Máximo do Agrupamento).	% do PSR total da análise de risco que pertence ao agrupamento (risco relativo).

#### 4.3.4.1.7.

#### Risco Total por Ameaça

Esta tabela apresenta a consolidação dos resultados por ameaça, representando uma abordagem alternativa de gerência de riscos. Para facilitar a elaboração de um plano de ação, os controles associados a cada ameaça são explicitados.

Tabela 11: Risco Total por Ameaça

Ameaça	PSR	Índice de Conformidade	Índice de Segurança
- Nome da Ameaça.	Índice de risco associado a ameaça (somatório do PSR dos controles).	(Número de Controles com a ameaça Implementados )x100/(Número Total de Controles com a ameaça).	(PSR da Ameaça)x100/(PSR Máximo da Ameaça).
Controle	Resposta	PSR Total	PSR Ameaça
Nome do controle que possui a ameaça.	Resposta dada ao controle (Implementado, Não Implementado ou Não se Aplica).	Índice de risco associado ao controle (somatório do PSR dos controles).	Índice de risco associado a ameaça (PSR Total/Número de Ameaças).

#### 4.3.4.1.8.

#### Risco Total por Checklist

Nesta tabela encontra-se a consolidação dos resultados por *checklist*, através do somatório do PSR de cada instância sua no projeto de avaliação. Estes dados podem ser utilizados no direcionamento dos recursos, através da identificação da área de processo, do papel ou da característica de tecnologia ou ambiente mais comprometida ou que representa maior risco ao projeto ou a organização.

Tabela 12: Risco Total por Checklist

Nome Checklist	PSR	Índice de Conformidade	Índice de Segurança	%PSR
Nome do checklists utilizado na avaliação.	Índice de risco associado a ameaça (somatório do PSR dos controles).	((Número de Controles Implementados)x100/(Número Total de Controles).	(PSR do Checklist)x100/(PSR Máximo do Checklist).	% do PSR total da análise de risco que pertence ao Checklist (risco relativo).

#### 4.3.4.1.9.

#### Situação dos Controles

Esta tabela é utilizada para o acompanhamento da avaliação, indicando o PSR atual, as evidências associadas e os comentários adicionados a cada ativo. Os elementos são agrupados pelo ativo e pelo *checklist*.

Tabela 13: Situação dos Controles

Agrupamento	Controle	PSR	Evidências	Comentário
- Ativo :				
- Checklist :				
Agrupamento ao qual pertence o controle.	Nome do controle.	Índice de risco associado ao controle (1 - 125).	Evidências da implementação do controle associadas durante a avaliação.	Comentários relativos a implementação do controle adicionados durante a avaliação.

#### **4.3.4.2. Gráficos**

##### **4.3.4.2.1. Risco por Agrupamento**

O gráfico de risco por agrupamento visualiza os resultados consolidados por área de processo e nível de capacidade e maturidade. A partir deste gráfico é possível identificar as áreas de processo com maior risco na organização e direcionar a aplicação dos recursos.

##### **4.3.4.2.2. Risco por Ameaça**

O gráfico de risco por ameaças fornece uma visualização geral das ameaças, permitindo que ameaças consideradas perigosas e que possuam um alto índice de risco possam ser identificadas e atacadas com prioridade.

##### **4.3.4.2.3. Risco dos Ativos**

O gráfico de risco nos ativos visualiza os resultados da análise de risco consolidados nos ativos, permitindo a rápida identificação dos ativos mais comprometidos e facilitando a execução de medidas pontuais para mitigação de riscos.

##### **4.3.4.2.4. Risco dos Objetivos do Negócio**

O gráfico dos objetivos de negócio permite a visualização da análise de risco consolidada nos dois níveis de objetivo, funcionando como base para a tomada de decisões estratégicas da organização, através da identificação dos objetivos mais comprometidos e dos *checklists* e controles que devem ser implementados para que o objetivo possa ser alcançado.

As tabelas e gráficos apresentados aqui consolidam os resultados da análise de risco e conformidade de formas diferentes, criando um rico conjunto de dados para a tomada de decisão. Neste trabalho tentou-se identificar um conjunto suficiente para a maioria dos cenários de avaliação, ficando a cargo da organização identificar e configurar tabelas e gráficos que atendam a necessidades e visualizações específicas.

#### 4.3.4.2.5. Relevância x Risco de Agrupamentos

Neste gráfico é possível visualizar os agrupamentos (áreas de processo) que possuem maior relação Relevância-Risco, permitindo uma seleção dos agrupamentos prioritários para a próxima iteração do ciclo de melhoria contínua. Este gráfico é dividido em quadrantes, como mostrado na Figura 14 abaixo. Os agrupamentos localizados no terceiro quadrante representam as áreas de processo mais comprometidas e com maior relevância para a organização, ou seja, estas áreas devem ser abordadas imediatamente. Os agrupamentos no primeiro quadrante representam as áreas de processo menos prioritárias e com menor risco associado, representando uma área confortável onde apenas refinamentos nos processos podem ser feitos e cujas áreas de processo só devem ser abordadas em último caso. Finalmente, os agrupamentos localizados no segundo e quarto quadrante representam as áreas de processo em um estado intermediário, onde uma análise mais elaborada deve ser feita para determinar quais áreas são prioritárias.

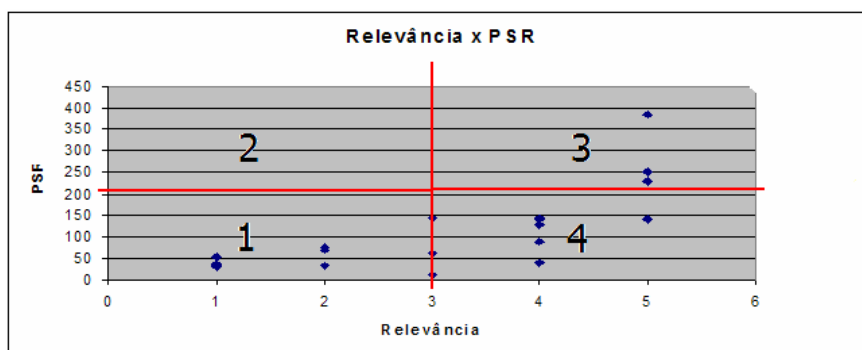


Figura 14: Gráfico Relevância x Risco de Agrupamentos

#### 4.3.4.2.6. Relevância x Risco de Objetivos do Negócio e Objetivos de TI

Estes gráficos possuem a mesma estrutura e interpretação do gráfico Relevância x Risco de Agrupamentos, fornecendo uma visão gerencial dos dados obtidos e podendo ser utilizados como base para a tomada de decisões estratégicas.

#### 4.3.4.2.7. Consolidação dos Resultados em Ativos, Objetivos do Negócio e Objetivos de TI

Este gráfico apresenta o mapeamento dos ativos da organização nos objetivos de TI e o mapeamento destes nos objetivos do negócio da organização.

Também são apresentados os resultados consolidados de risco e conformidade em cada nível, como pode ser visto na Figura 15.

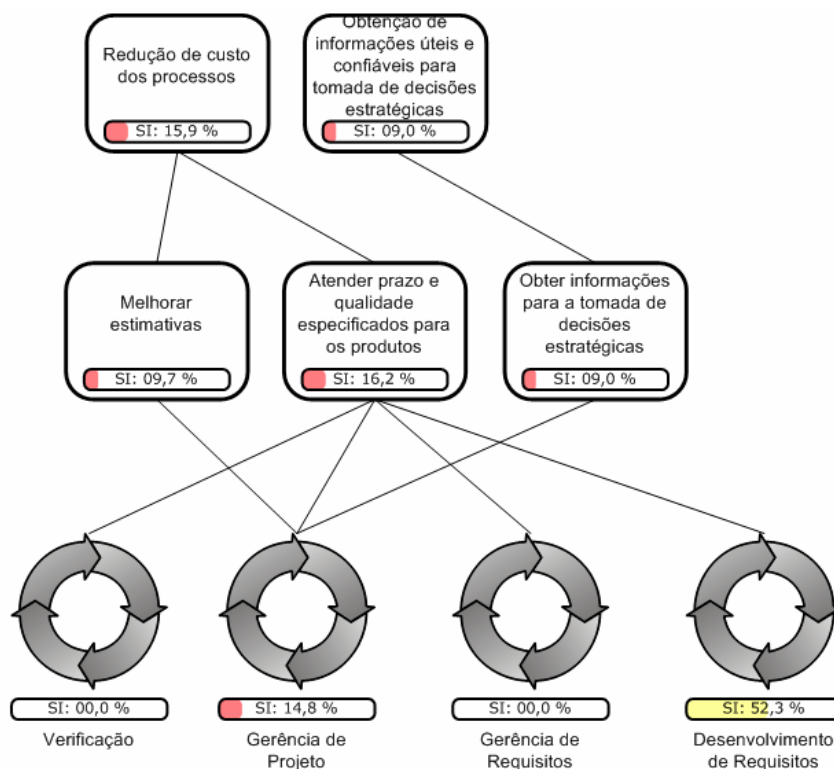


Figura 15: Gráfico de Consolidação dos Resultados em Ativos, Objetivos do Negócio e Objetivos de TI

Este gráfico fornece uma visão geral dos resultados da avaliação, permitindo identificar como um nível contribui com o risco e a conformidade dos demais.

#### 4.3.5. Relatórios

##### 4.3.5.1. Relatório Operacional de Risco

O relatório operacional de risco é gerado de forma automática pela ferramenta Check-up Tool, consolidando os resultados da análise de risco e conformidade nos controles. Este relatório apresenta os controles não implementados, organizados por agrupamento e ordenados pelo índice PSR, utilizando o seguinte formato:



Tabela 14: formato de apresentação de dados do Relatório Operacional de Risco

Controle	PSR®	Detalhes	Ativo
Nome do controle verificado	Somatório do PSR dos controles preenchidos como "Não Implementado" durante a avaliação.	Justificativa (Porque?)  Justificativa do controle.	<b>** Tipo_Ativo **</b>  Lista de todos os ativos de um determinado tipo que tiveram o controle preenchido como "Não Implementado" - Índice PSR associado ao controle na avaliação do ativo
		Recomendação (Como?)  Recomendação de implementação do controle. <b>Referências</b> Referências para a implementação do controle  <b>Checklist</b> Checklist ao qual o controle pertence	
		<b>Comentários</b> Comentários associados ao controle durante a realização da avaliação.	

Através dos dados contidos neste relatório é possível:

- Identificar inconsistências no preenchimento dos *checklists*: Controles verificados em tipos de ativos distintos com resultados muito diferentes;
- Obter uma visão geral dos resultados da avaliação: Resultados dos controles mais os dados de como eles foram preenchidos (ativos onde ele não está implementado, com a sua participação no risco, e comentários);
- Visualizar o estado de implementação dos controles em cada ativo avaliado;
- Derivar um plano de ação através da identificação dos controles com maior risco associado (maior índice PSR) e utilização da recomendação e referências para a implementação dos controles.

Ao longo deste trabalho o conteúdo deste relatório foi customizado para o domínio de processos de desenvolvimento de software, através da adequação do seu conteúdo estático.

#### 4.3.5.2. Relatório de Análise de Risco

O relatório de análise de risco constitui o relatório final da avaliação, fornecendo um conjunto de gráficos, tabelas, interpretações e sugestões que, junto

com os gráficos e tabelas citados acima, constitui uma base de dados fundamental para a tomada de decisões. Este relatório é composto por cinco partes, sendo elas:

- **Sumário Executivo** contextualiza a análise realizada, apresentando o método utilizado para verificação e cálculo de risco e definindo termos relevantes.
- **Principais Conclusões** apresenta uma visão geral dos resultados obtidos e visões detalhadas dos resultados consolidados por ativo e agrupamento. Nesta seção os principais dados para a tomada de decisão são apresentados e sugestões de abordagens para o direcionamento de recursos e implantação de um plano de ação são apresentadas (orientação pelos ativos de maior risco ou menor conformidade; componentes de negócio com maior risco ou menor conformidade; agrupamentos com maior risco ou menor conformidade; ameaças com maior risco).
- **Escopo da Análise** apresenta o escopo da análise realizada, indicando os perímetros avaliados, os ativos verificados, os *checklists* preenchidos ao longo da avaliação e a equipe responsável pela avaliação.
- **Análise de Risco Consolidada** apresenta consolidações dos resultados obtidos em um nível gerencial, através da visualização dos riscos e conformidade por objetivos de negócio (objetivos do negócio e objetivos de TI), riscos por ameaça, risco e conformidade por ativo e tipo de ativo (Processo, Pessoa, Ambiente e Tecnologia), distribuição dos riscos pelos ativos e tipos de ativo (ativos e tipos de ativo com risco classificado como Muito Baixo, Baixo, Médio, Alto e Muito Alto) e risco por perímetro da organização avaliado. Os dados contidos nesta seção servem como um apoio para a tomada de decisão e elaboração de um plano de ação para diminuir o risco e/ou aumentar a conformidade nas áreas críticas identificados na seção Principais Conclusões.
- **Risco por Componente de Negócio** apresenta uma visão mais detalhada dos resultados consolidados pelos objetivos de negócio e de TI da organização, visualizando os componentes do risco e da conformidade em cada objetivo.

Ao longo deste trabalho o conteúdo estático e dinâmico deste relatório foi customizado para o domínio de processos de desenvolvimento de software.

#### **4.3.6.**

#### **Determinação da Severidade dos Controles**

Para tentar diminuir a subjetividade da determinação da severidade dos controles, foi desenvolvida uma abordagem baseada no impacto de cada ameaça para a organização.

O primeiro passo para a determinação da severidade consiste em atribuir um nível de um (mais baixo) a cinco para cada ameaça, considerando-se o cenário da organização. Em seguida, os controles são elaborados e as ameaças associadas. Finalmente, a severidade do controle é determinada pelo piso da média das severidades das ameaças associadas ao controle.

Com a utilização desta abordagem, o desenvolvimento dos controles não fica propenso a classificações de severidade inconsistentes entre *checklists* desenvolvidos por equipes distintas, facilitando o desenvolvimento colaborativo. Outra vantagem é que a severidade de um controle irá representar uma visão organizacional dos riscos e não mais uma visão restrita ao *checklists*.

#### **4.3.7.**

#### **Preenchimento dos Controles**

Tendo em vista que a grande maioria dos métodos de avaliação de processos de desenvolvimento (SCAMPI, MA-MPS, ISO/IEC 15504) utiliza uma estrutura de níveis para a classificação da implementação de uma diretiva do modelo ou norma, e que a estrutura da ferramenta Check-up Tool define apenas as categorias “Implementado” e “Não Implementado”, foi desenvolvida uma abordagem para que controles parcialmente implementados fossem classificados.

Partindo do fato de que um controle parcialmente implementado não se encontra implementado, foi determinado que, quando a análise realizada indicasse que um controle não foi totalmente atendido, este deve ser preenchido como “Não implementado”. Utilizando a segunda premissa de que um controle parcialmente implementado possui uma probabilidade menor de causar danos do que um controle não implementado, foi determinado que, para cada nível de implementação atingido pelo controle, a sua probabilidade será diminuída em uma unidade, até chegar ao valor mínimo 1.

Para exemplificar a abordagem, considere um controle cuja probabilidade seja quatro. Em uma avaliação MPS.BR, um controle classificado como parcialmente implementado será preenchido como Não Implementado e a sua probabilidade será alterada para três. O mesmo ocorre para um controle considerado Largamente Implementado, sendo que, neste caso, a probabilidade seria alterada para dois.

O resultado desta abordagem é que, ao final da análise de risco, os controles parcialmente implementados contribuirão com menos risco do que os controles do mesmo tipo classificados como não implementados.

#### **4.3.8. Identificação dos Objetivos do Negócio**

A última customização realizada funciona mais como um apoio à realização de avaliações do que uma adaptação da ferramenta e da sua forma de utilização. Baseando-se no COBIT (ITGI, 2005), foi elaborada uma lista de objetivos do negócio e de TI, que representa uma entrada de dados inicial para estes parâmetros. Dessa forma, a atividade de definição dos objetivos que guiarão a avaliação passa de um trabalho exaustivo de identificação para uma simples seleção. A lista completa com os objetivos gerada é apresentada no Apêndice D.