

MAPEANDO A NORMA DE GERENCIAMENTO DE RISCOS AS/NZS 4360 NO PMBOK

Marcelo Gil Aldenucci (PUCPR)
mgaldenucci@yahoo.com

Luiz Marcio Spinosa (PUCPR)
m.spinosa@pucpr.br

Fábio Favaretto (PUCPR)
professor.favaretto@gmail.com



O Project Management Body of Knowledge (PMBOK) é um guia de conhecimentos amplamente empregado na indústria para guiar a concepção e a implementação de processos de gerenciamento de projetos. De maneira semelhante, a norma AS/NZS 4360 estabelece critérios para o desenvolvimento de processos de gerenciamento de riscos. No entanto, não há evidência de que ambos sejam compatíveis. Este artigo descreve uma pesquisa onde os aspectos críticos da norma foram identificados e mapeados no PMBOK. Foi verificado que este implementa plenamente cerca de 63% dos fatores críticos de aderência a norma e que não há nenhuma incompatibilidade entre ambos. As conclusões contribuem para direcionar os esforços de elaboração de processos de gerenciamento de riscos em projetos.

Palavras-chaves: Gerenciamento de riscos, Gerenciamento de projetos, PMBOK, AS/NZS 4360

1. Introdução

A disciplina de gerenciamento de projetos ocupa-se de estudar os mecanismos através dos quais um projeto pode ser administrado, considerando aspectos como cronograma, custo, emprego de recursos e qualidade. Neste contexto, numerosos riscos emergem conforme o desenrolar da atividade, tais como não atendimento a prazos e orçamentos. Considerando estes fatores, entende-se que o gerenciamento de projetos deve se ocupar também do gerenciamento dos riscos que os envolvem.

O *Project Management Body of Knowledge* (PMBOK), publicado pelo *Project Management Institute* (PMI), é um guia de conhecimentos de gerenciamento de projetos amplamente empregado na indústria para guiar a concepção e a implementação de processos relacionados a este tema. Tal guia possui um capítulo dedicado ao gerenciamento de riscos, que apresenta métodos, técnicas e melhores práticas relacionadas à área.

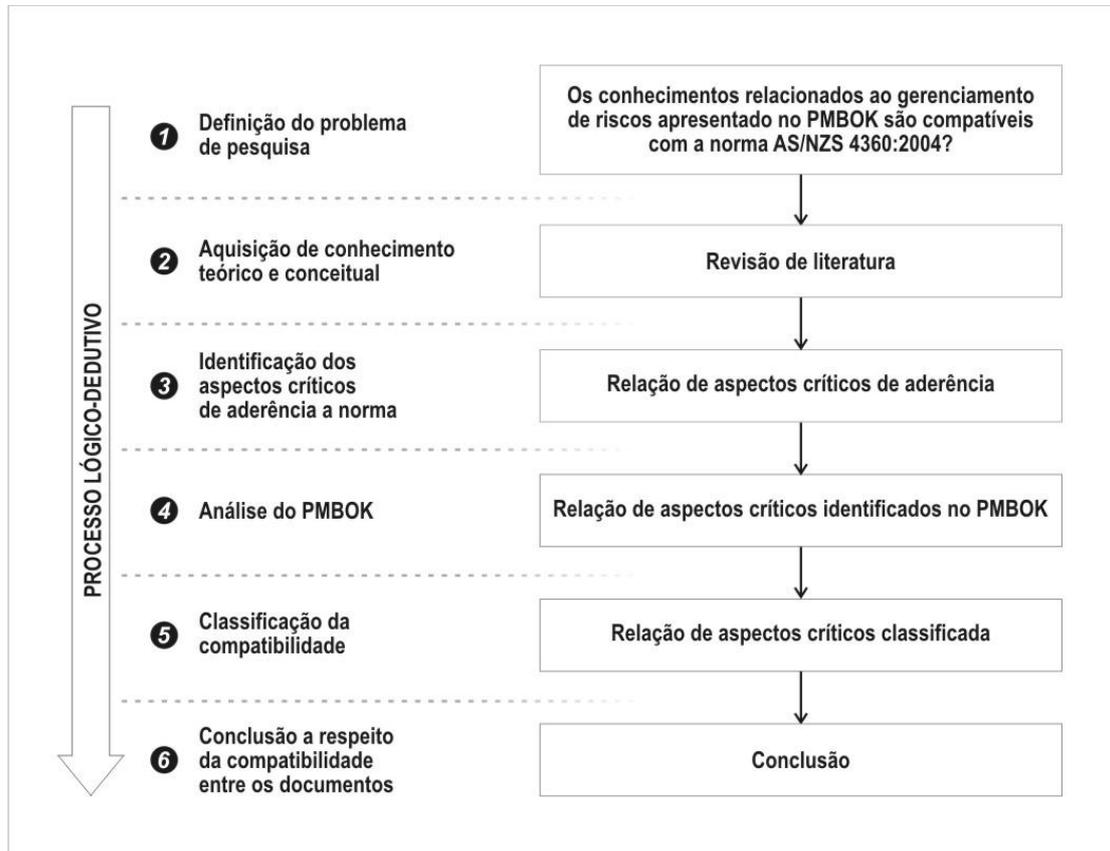
Paralelamente, o gerenciamento de riscos é aplicado em diversas áreas do conhecimento, e, apesar de ainda não existirem normas internacionais a respeito, uma norma regional australiana e neozelandesa, a AS/NZS 4360 (2004) é geralmente adotada como referência nas implementações de processos de gerenciamento de riscos. Considerando que a AS/NZS 4360 é uma norma de gerenciamento de riscos amplamente aceita, espera-se que uma eventual norma internacional na área possua o mesmo formato (MAYER, 2008).

O PMBOK não faz referência expressa à norma, e, portanto, não há garantia de compatibilidade entre ambos. Esta situação cria um problema: o PMBOK é compatível com a norma AS/NZS 4360? O objetivo deste trabalho é, portanto, identificar os aspectos críticos da norma presentes no PMBOK, concluindo se os processos descritos na obra do PMI são aderentes ou compatíveis a ela ou não. Cabe aqui fazer uma distinção entre os termos empregados neste artigo: por “aderência”, entende-se que uma implementação de todos os requisitos está presente; por “compatibilidade”, entende-se que não existem práticas que impossibilitem a execução de determinados requisitos. A conclusão pretendida proporcionará uma contribuição para as organizações interessadas em conceber seus processos de gerenciamento de riscos em projetos direcionarem seus esforços, corroborando, ou não, o corpo de conhecimentos do PMI frente a instituições de normatização. Por exemplo, uma organização que execute processos desenhados de acordo com o PMBOK poderá estimar o esforço necessário para a adequação à norma.

Este trabalho está organizado da seguinte maneira: a seção 2 apresenta a estratégia de pesquisa adotada para a condução do trabalho, com vistas a promover um caráter científico; A seção 3 apresenta uma breve revisão da literatura acerca do gerenciamento de riscos em projetos; a seção 4 apresenta uma visão geral acerca de alguns modelos, normas e padrões de gerenciamento de risco, considerando o escopo proposto para o trabalho; a seção 5 mostra o trabalho realizado, com o relacionamento entre os aspectos identificados na AS/NZS 4360 e no PMBOK; a seção 6 apresenta a conclusão quanto à compatibilidade entre o PMBOK e a norma AS/NZS 4360; e, ao final, é apresentada a relação de referências utilizadas.

2. Estratégia de pesquisa

Considerando que, conforme observado por Lakatos e Markoni (2005), “não há ciência sem o emprego de métodos científicos”, uma estratégia de pesquisa essencialmente lógico-dedutiva foi traçada para guiar a execução do trabalho. A Figura 1 apresenta esta estratégia.



Fonte: Elaborado pelo autor

Figura 1 – Estratégia de pesquisa

Na Fase 1 o problema de pesquisa é delimitado à seguinte questão: “Os conhecimentos relacionados ao gerenciamento de riscos apresentado no PMBOK são compatíveis com a norma AS/NZS 4360:2004”? A Fase 2 concretiza-se com a revisão de literatura apresentada na seção 3 deste artigo. A identificação dos aspectos críticos da norma e a análise crítica do PMBOK em busca destes aspectos (Fase 3 e Fase 4) é relatada na seção 5. O critério adotado para considerar determinado aspecto como “crítico” na norma é o emprego de termos que determinem a obrigação ou recomendação explícita de sua execução, tais como “deve-se”, “é necessário” e “recomenda-se”. Uma vez identificados todos estes fatores, o PMBOK é analisado criticamente buscando-se sua identificação. Esta análise possibilita três conclusões: compatível; compatível, mas não aderente; e incompatível.

3. Gerenciamento de Riscos em Projetos

Embora alguns autores considerem um risco apenas como “uma possibilidade de sofrer uma perda” (DOROFEE et al, 1996), em todos os tipos de empreendimentos existem eventos potenciais e conseqüências que constituem oportunidades de benefícios (positivas) ou ameaças ao sucesso (negativas). Desta forma, o gerenciamento de riscos é crescentemente reconhecido como estando preocupado tanto com os aspectos positivos como os negativos dos riscos (AIMIRC, 2002).

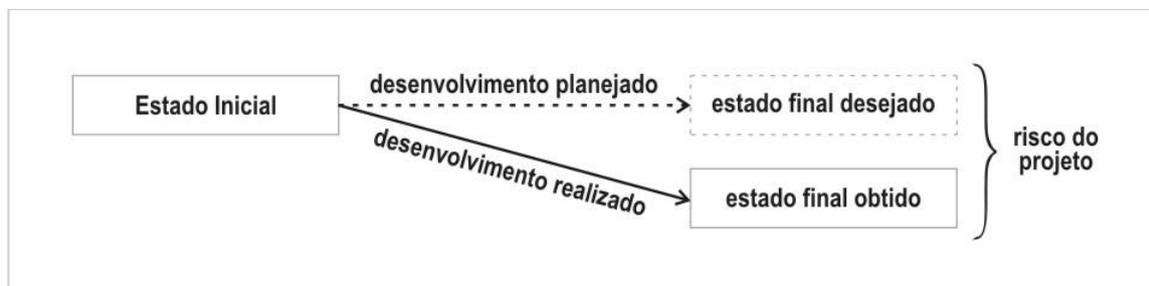
A disciplina de gerenciamento de riscos é aplicada nas mais variadas áreas do conhecimento, e em cada uma delas, o termo *risco* assume uma definição diferente, de acordo com o

contexto (KLOMAN, 1990). Neste cenário, Charette (1990) aponta três elementos que estão sempre presentes na definição de um risco:

- A existência de uma perda potencial;
- A incerteza acerca do resultado em caso de materialização do risco;
- A necessidade de tomar alguma decisão para lidar com a incerteza.

Já a ISO/IEC (2002) define um risco como “a combinação da probabilidade de ocorrência de um evento e suas conseqüências”. Abordagem semelhante é empregada pelo PMI (2008), que diz que um risco “é uma condição incerta que, se ocorrer, terá um efeito positivo ou negativo sobre pelo menos um objetivo do projeto, como tempo, custo, escopo ou qualidade”. Esta proposição vai de encontro às demais definições apresentadas pelo PMI (2008), de que um projeto é “um empreendimento temporário para criar um produto, serviço ou resultado único”, e que o gerenciamento de projetos é “a aplicação de conhecimentos, habilidades, ferramentas e técnicas nas atividades do projeto para atender seus requisitos”. Desta forma, entende-se que as demandas concorrentes envolvidas neste processo provocam o surgimento de diferentes riscos, que devem ser gerenciados com vistas ao atendimento dos requisitos do projeto.

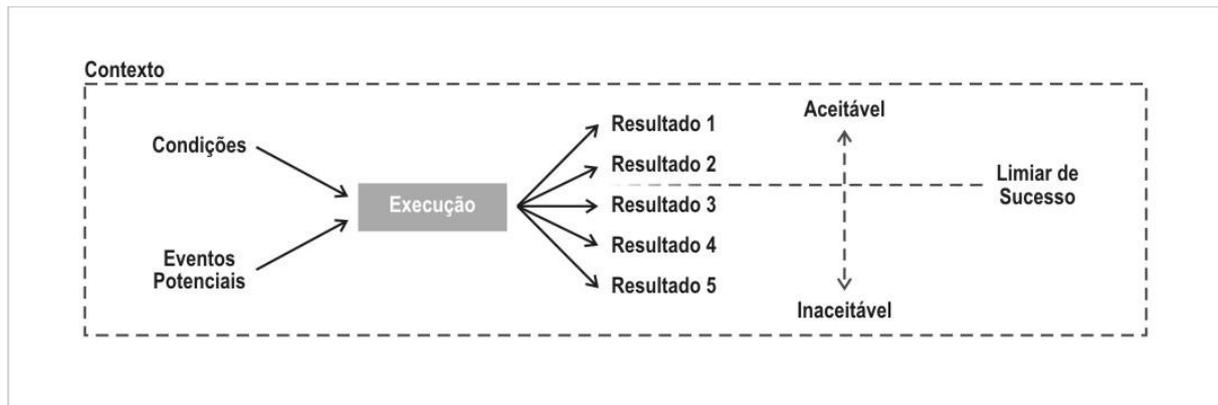
Marcelo-Cocho (2007) indica a existência de dois estados fundamentais que caracterizam um projeto em relação aos seus riscos: o “estado final desejado” (EFD) e o “estado final atingido” (EFA). O caminho que leva ao EFD é o planejado para o projeto, enquanto que o caminho que leva ao EFA é efetivamente realizado, conforme mostra a Figura 2. Marcelo-Cocho (2007) argumenta que a diferença entre o planejado e o realizado compreende os riscos do projeto, e que a função do gerenciamento de riscos do projeto é limitar a diferença entre o EFD e o EFA.



Fonte: Adaptado de Marcelo-Cocho (2007)

Figura 2 – O resultado de um projeto visto como um derivado de seu objetivo

Conforme SEI (2007), um projeto tem um espectro de possíveis resultados, alguns aceitáveis e outros não, de acordo com os requisitos e as expectativas dos *stakeholders*. O limiar de atendimento a estes requisitos e expectativas é o que define o sucesso ou não do projeto, conforme a Figura 3.



Fonte: Adaptado de SEI (2007)

Figura 3 – Limiar de sucesso do projeto

O resultado é diretamente influenciado por duas variáveis principais: condições correntes e eventos potenciais. Desta forma, o gerenciamento de riscos se incube, também, da projeção de possíveis cenários de acordo com estas variáveis, empregados na elaboração do plano de gerenciamento de riscos. SEI (2007) aponta alguns elementos que devem ser levados em consideração no momento da composição de tais cenários:

- Contexto: É a situação e o ambiente no qual um processo é executado (logo, é a base de informações e conhecimentos iniciais sobre a qual serão determinados os riscos);
- Execução: É o que está sendo feito para se atingir os objetivos;
- Condições: São as circunstâncias que direta ou indiretamente afetam o resultado, como restrições ou premissas;
- Eventos potenciais: São ocorrências imprevisíveis que, combinadas a determinadas condições podem impactar – positiva ou negativamente – algum resultado esperado;
- Espectro de resultados potenciais: É o conjunto de possibilidades de resultados para o projeto.

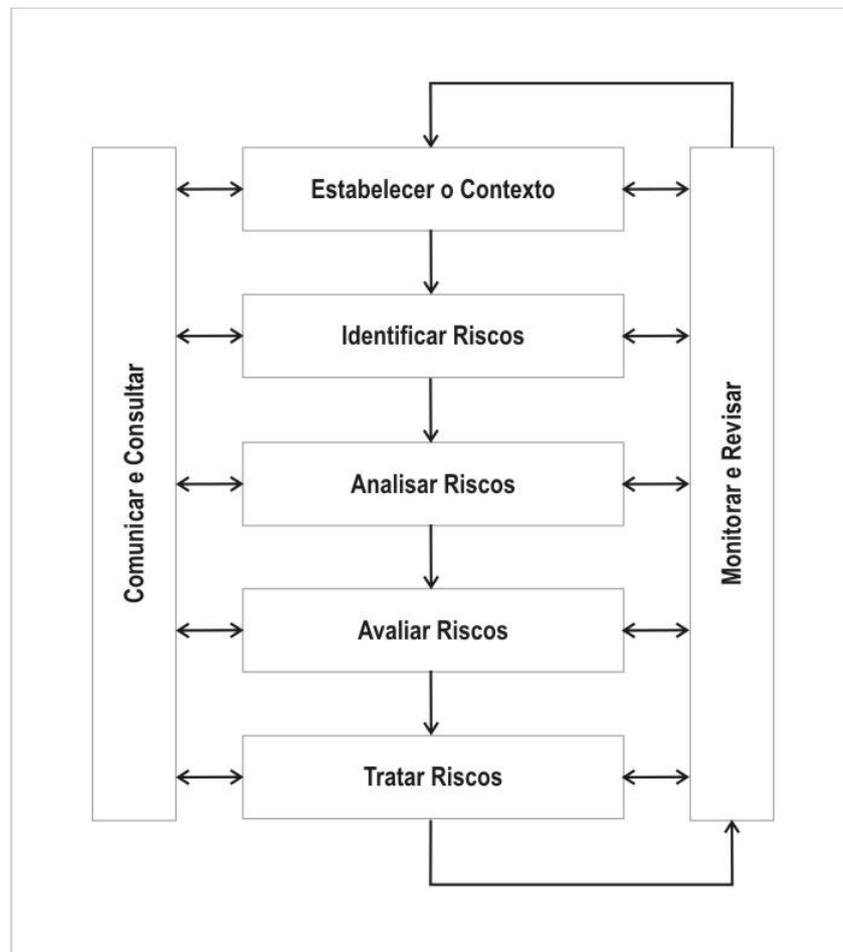
O gerenciamento de riscos tem, então, a função de manter um nível aceitável de confiança de que os resultados do projeto estão acima do limiar de sucesso.

Como é possível notar, através das atividades desenvolvidas e divulgadas pelo SEI (CMM, 2002; SEI, 2006; SEI, 2007), as pesquisas na área de gerenciamento de riscos em projetos são especialmente importantes quando relacionadas a projetos de software. Modelos de processo de software, tais como o CMMI-SW (CMM, 2002) e o RUP (RATIONAL, 2003) geralmente contemplam aspectos do gerenciamento de riscos. Rocha (2004) aponta que os processos de gerenciamento de riscos apresentados pelo PMBOK, CMMI-SW e RUP são compatíveis entre si, sendo que os apresentados pelo PMBOK são mais completos e abrangentes, já que não são específicos para a indústria de software.

4. Normas, Padrões e Modelos no Gerenciamento de Riscos

Não existe nenhuma norma internacional completa a respeito de gerenciamento de riscos. Em março de 2009 a futura norma ISO 31000 está em fase de desenvolvimento (ISO, 2009), com previsão de publicação ainda em 2009. Conforme Mayer (2008), espera-se que esta norma seja aderente a já estabelecida AS/NZS 4360 (2004).

A AS/NZS 4360 possui a premissa de ser aplicável em qualquer situação de gerenciamento de riscos em qualquer tipo de organização, sem se restringir a um segmento específico. Ela apresenta um glossário com os principais termos empregados, uma visão geral do processo de gerenciamento de riscos, um detalhamento do objetivo de cada etapa do processo e indicações de como estabelecer um gerenciamento de riscos efetivo. A Figura 4 apresenta o relacionamento entre os diferentes processos de gerenciamento de riscos sugeridos pela norma.



Fonte: Adaptado de AS/NZS (2004)

Figura 4 – Interação entre os processos da norma AS/NZS 4360

Em relação aos riscos em projetos, a referência amplamente utilizada é o PMBOK, que além de melhores práticas em relação ao gerenciamento de riscos em projetos apresenta práticas relacionadas a outras áreas, tais como escopo, tempo e recursos humanos. Com relação aos riscos, o PMI (2008) estabelece seis atividades principais:

- Planejar o gerenciamento de riscos;
- Identificar riscos;
- Realizar análise qualitativa de riscos;
- Realizar análise quantitativa de riscos;
- Planejar as respostas aos riscos;
- Monitorar e controlar riscos.

Esses processos devem ser executados iterativamente ao longo do ciclo de vida do projeto, gerando uma série de documentos, tais como o Plano de gerenciamento de riscos do projeto e o Registro de riscos.

5. Mapeando a Norma AS/NZS 4360 no PMBOK

Em linha com o objetivo apresentado na introdução deste artigo, espera-se obter o entendimento de como os principais aspectos da norma AS/NZS 4360:2004 estão presentes no PMBOK, e, desta forma, concluir se este é aderente à norma ou não.

Em uma primeira análise, é possível verificar que, em linhas gerais, as etapas do processo estabelecidas na norma e no PMBOK são semelhantes, embora não idênticas, conforme comparação apresentada na Tabela 1.

AS/NZS 4360	PMBOK
Estabelecer o contexto	Planejar o gerenciamento de riscos
Identificar riscos	Identificar riscos
Analisar riscos	Realizar análise qualitativa de riscos Realizar análise quantitativa de riscos
Avaliar riscos	-
Tratar riscos	Planejar as respostas aos riscos
Comunicar e consultar	Gerenciamento das comunicações do projeto / Reportar a performance
Monitorar e revisar	Monitorar e controlar riscos

Fonte: Elaborado pelo autor.

Tabela 1 – Comparação entre as etapas estabelecidas pela AS/NZS 4360 e PMBOK

Para um detalhamento do trabalho, para cada uma das etapas listadas acima foram identificados os aspectos críticos de aderência, conforme a Tabela 2.

#	Aspecto crítico na AS/NZS 4360	Análise PMBOK	Conclusão
1	O processo de gerenciamento de riscos é genérico e independente de qualquer indústria ou setor econômico específico, sendo que sua concepção e implementação deve ser adaptada para as necessidades de cada organização.	Aderente, já que o PMBOK considera quaisquer tipos de projetos, sem discriminar uma área de aplicação específica.	Compatível.
2	O gerenciamento de riscos aplica-se tanto ao gerenciamento de potenciais perdas quanto ganhos.	Aderente, já que o PMBOK considera que “Os objetivos do gerenciamento de riscos do projeto são aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos ao projeto”.	Compatível.
3	O gerenciamento de riscos é parte integrante da boa administração. É um processo iterativo de melhoria contínua.	O PMBOK não explicita o caráter iterativo dentro de um mesmo projeto, mas indica a necessidade de execução em todo projeto, o que sugere a melhoria contínua: “Cada processo [de gerenciamento de riscos do projeto] ocorre pelo menos uma vez em todos os projetos e também em uma ou mais fases do projeto, se ele estiver dividido em fases”.	Compatível.
4	Comunicar e consultar <i>stakeholders</i>	O PMBOK prevê a confecção de	Compatível, mas

#	Aspecto crítico na AS/NZS 4360	Análise PMBOK	Conclusão
	internos e externos conforme apropriado em cada estágio do processo de gerenciamento de riscos como um todo.	relatórios de desempenho ao longo do processo de gerenciamento de riscos, com divulgação aos interessados previamente definidos. No entanto, não menciona explicitamente a necessidade de comunicar fatos relacionados ao gerenciamento de riscos.	para estabelecer a aderência à norma necessita de ampliações.
5	É importante desenvolver um plano de comunicação tanto para <i>stakeholders</i> internos quanto externos no primeiro estágio do processo. Este plano deve endereçar aspectos relacionados ao próprio risco e ao processo de gerenciamento.	Idem anterior.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
6	A percepção de risco dos <i>stakeholders</i> deve ser levada em consideração no processo de tomada de decisão.	O PMBOK indica que os fatores ambientais da empresa devem ser levados em consideração no planejamento do gerenciamento de riscos. Isto inclui as atitudes e tolerâncias dos <i>stakeholders</i> .	Compatível.
7	Estabelecer o contexto externo, interno e de gerenciamento de riscos no qual o resto do processo ocorrerá. O critério contra o qual os riscos serão avaliados deve ser estabelecido e a estrutura da análise definida.	A etapa de planejamento do gerenciamento de riscos delimitada no PMBOK contempla os fatores ambientais da empresa (internos) e ativos de processos organizacionais. No entanto, não determina explicitamente que fatores externos devam ser considerados também.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
8	Definir o escopo do processo de gerenciamento de riscos, considerando o ambiente interno e externo a organização, o propósito da atividade de gerenciamento de riscos e considerações a respeito da interface entre os ambientes interno e externo.	Idem anterior.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
9	Os objetivos, metas, estratégias, escopo e parâmetros da atividade ou parte da organização para a qual o processo de gerenciamento de risco está sendo aplicado devem ser estabelecidos, assim como os recursos necessários e registros a serem mantidos.	O processo de gerenciamento do escopo do projeto se ocupa destas tarefas.	Compatível.
10	Subdividir o projeto em um conjunto de elementos ou passos visando prover um <i>framework</i> lógico para a análise dos riscos.	Idem anterior. O PMBOK trata esse conjunto de elementos como uma Estrutura Analítica do projeto (EAP).	Compatível.
11	Identificar onde, quando, porque e como eventos podem prevenir, degradar, atrasar ou melhorar a capacidade de atingir os objetivos.	A atividade de Identificação de riscos ocupa-se destas tarefas.	Compatível.
12	A identificação de riscos deve incluir fatores dentro e fora do controle da organização.	Idem acima.	Compatível.
13	A identificação de riscos deve considerar possíveis causas e cenários.	Este aspecto não é explicitamente determinado pelo PMBOK.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
14	Identificar e avaliar os controles	Este aspecto não é explicitamente	Compatível, mas

#	Aspecto crítico na AS/NZS 4360	Análise PMBOK	Conclusão
	existentes. Determinar conseqüências e probabilidades e, então, o nível de risco. Essa análise deve considerar o espectro de potenciais conseqüências e como elas podem ocorrer.	determinado pelo PMBOK.	para estabelecer a aderência à norma necessita de ampliações.
15	Identificar os processos, mecanismos ou práticas existentes para minimizar riscos negativos e potencializar riscos positivos.	Este aspecto não é explicitamente determinado pelo PMBOK.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
16	Conseqüência e probabilidade são combinadas para produzir um nível de risco.	A atividade de Análise quantitativa de riscos ocupa-se destas tarefas.	Compatível.
17	A análise qualitativa usa palavras para descrever a magnitude das conseqüências potenciais e a probabilidade dessas conseqüências se materializarem.	Idem acima.	Compatível.
18	A análise quantitativa usa números para descrever a magnitude das conseqüências potenciais e a probabilidade dessas conseqüências se materializarem.	A etapa de Análise quantitativa dos riscos do PMBOK emprega números para descrever a criticidade do risco.	Compatível.
19	Análise de sensibilidade deve ser empregada para adequar as estimativas quantitativas de análise de riscos.	O PMBOK indica o emprego de análise de sensibilidade na análise quantitativa dos riscos.	Compatível.
20	Comparar níveis estimados de risco contra critérios pré-estabelecidos e considerar o saldo entre benefícios potenciais e resultados adversos. Isso possibilita tomadas de decisão em relação ao tratamento necessário e priorização.	A comparação contra uma linha base de riscos não é explícita no PMBOK.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
21	Os objetivos da organização e a extensão da oportunidade / ameaça resultante devem ser consideradas.	Contemplado pelas etapas de Identificação dos riscos do projeto e Análise qualitativa dos riscos do PMBOK.	Compatível.
22	Desenvolver e implementar estratégias específicas e efetivas em relação a seu custo, e planos de ação para aumentar os benefícios potenciais e reduzir os custos potenciais.	Contemplado pela etapa de Planejamento de resposta aos riscos.	Compatível.
23	Selecionar a opção de tratamento mais apropriada envolve balancear os custos de implementação com os benefícios derivados.	Característica não identificada explicitamente no PMBOK.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
24	As opções de tratamento dos riscos devem considerar os valores e percepções dos stakeholders e as maneiras mais apropriadas de estabelecer comunicação com eles.	Idem acima.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
25	O próprio tratamento dos riscos pode incluir novos riscos, que devem, eles mesmos, serem identificados, avaliados, tratados e monitorados.	Idem acima.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
26	O plano de tratamento dos riscos deve	Contemplado pelo Plano de	Compatível.

#	Aspecto crítico na AS/NZS 4360	Análise PMBOK	Conclusão
	incluir: ações propostas, recursos requeridos, responsabilidades, cronograma, medidas de performance e requerimentos de reporting e monitoramento.	gerenciamento dos riscos.	
27	É necessário monitorar e revisar a efetividade de todos os passos do processo de gerenciamento de riscos.	Contemplado pela etapa de Monitoramento e controle dos riscos.	Compatível.
28	É necessário repetir o ciclo de gerenciamento de riscos regularmente.	O processo de Gerenciamento de riscos do projeto é iterativo.	Compatível.
29	Comparar o progresso realizado contra o previsto no plano de gerenciamento de riscos.	Contemplado pela etapa de Monitoramento e controle dos riscos.	Compatível.
30	Registrar lições aprendidas.	Prática implementada pela etapa de Fechamento do projeto.	Compatível.
31	Cada estágio do processo de gerenciamento de riscos deve ser registrado adequadamente, incluindo: pressupostos, métodos, fontes de dados, análises, resultados e razões para as decisões tomadas. As decisões em relação a manutenção de registros devem considerar requisitos legais e de negócio, o custo de criar e manter os registros os benefícios de reutilização de informações.	Não contemplado completamente pelo PMBOK.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
32	A organização deve desenvolver uma política de gerenciamento de riscos.	Não contemplado completamente pelo PMBOK.	Compatível, mas para estabelecer a aderência à norma necessita de ampliações.
33	Antes de iniciar o desenvolvimento de um plano de gerenciamento de riscos, a organização deve avaliar criticamente suas práticas e processos de modo a identificar elementos de gerenciamento de riscos já estabelecidos.	Contemplado na etapa de Planejamento do gerenciamento de riscos do projeto, onde os ativos de processos organizacionais são levados em consideração.	Compatível.
34	O processo de gerenciamento de riscos deve ser customizado para cada organização.	O PMBOK fornece melhores práticas, e não um processo definido, o que demanda sua customização no momento da implementação.	Compatível.
35	A organização deve identificar os requisitos de recursos para o gerenciamento de riscos.	Contemplado pelos processos de gerenciamento dos custos do projeto.	Compatível.

Fonte: Elaborado pelo autor.

Tabela 2 – Mapeamento dos aspectos críticos de aderência a AS/NZS 4360 no PMBOK

6. Conclusão

Este artigo apresentou um estudo a respeito de dois padrões de gerenciamento de riscos distintos, o PMBOK e a norma AS/NZS 4360. Foram identificados os aspectos críticos de aderência à norma, e, para cada um deles, buscou-se equivalente no PMBOK, com vistas à identificação da compatibilidade.

Foram identificados 35 aspectos críticos relacionados à norma AS/NZS 4360 e, destes, 22 foram identificados plenamente no PMBOK, conforme a Tabela 3.

Conclusão	Quantidade	Percentual
Compatível	22	63%
Compatível, mas para estabelecer a aderência à norma necessita de amplificações.	13	37%
Incompatível	0	0%

Fonte: Elaborado pelo autor.

Tabela 3 – Conclusão em relação à aderência do PMBOK à norma AS/NZS 4360

Foi verificado que para aspectos como a consideração de fatores externos a organização e o balanceamento entre custos e benefícios obtidos, a norma mostra-se mais abrangente. No entanto, não existem elementos que indiquem incompatibilidade entre ambos, o que faz acreditar que uma organização que execute seus processos de acordo com os preceitos do PMI terá facilidade em adaptar-se ao atendimento à norma AS/NZS 4360, requerendo, para tanto, um esforço moderado (37% dos fatores críticos precisam ser implementados).

Considerando o estudo de Rocha (2004), é possível, ainda, estender este entendimento para o âmbito do desenvolvimento de software, já que aquele conclui que o processo de gerenciamento de riscos do PMBOK é compatível com o CMMI-SW e com o RUP. Cabe aqui, então, a sugestão de um futuro trabalho contemplando a verificação direta da aderência do CMMI e do RUP à norma AS/NZS 4360.

Referências

AIMIRC - The Association of Insurance and Risk Management; ALARM – The National Forum for Risk Management in the Public Sector; IRM – The Institute of Risk Management. *A Risk Management Standard.* Londres: 2002.

AS/NZS – Standards Australia/Standards New Zealand. *AS/NZS 4360:2004 Risk Management.* Sydney: AS, 2004.

CHARETTE, R. N. *Application Strategies for Risk Analysis.* New York, NY: McGraw-Hill Book Company, 1990.

CMMI Product Team. *CMMI for Systems Engineering/Software Engineering, Version 1.1 Staged Representation (CMU/SEI-2002-TR-029, ESC-TR-2002-029).* Pittsburgh, PA: Software Engineering Institute. Carnegie Mellon University, 2002.

DOROFEE, A.; WALKER, J.; ALBERTS, C.; HIGUERA, R.; WILLIAMS, R. *Continuous Risk Management Guidebook.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996.

ISO – The International Organization for Standardization. *ISO/FDIS 31000 General Information.* Disponível on-line em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170. Última consulta em 26 de março de 2009.

ISO/IEC – The International Organization for Standardization and the International Electrotechnical Commission. *ISO/IEC Guide 73:2002 Risk Management – Vocabulary – Guidelines for use in standards.* Geneve: ISO, 2002.

KLOMAN, H. F. *Risk Management Agonists.* Risk Analysis Vol. 10, n.2, p.201-205, junho, 1990.

LAKATOS, E. M. & MARKONI, M. *A Fundamentos de Metodologia Científica, 6ed.* São Paulo: Atlas, 2005.

MARCELO-COCHO, J. & FERNANDÉZ-DIEGO, M. *Risks and Project Management.* European Journal for the Informatics Professional, Vol. VIII, n 5, p. 36-41, outubro, 2007.

MAYER, J & FAGUNDES, L. L. *Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação.* Anais do VIII Simpósio Brasileiro em Segurança da Informação

e de Sistemas Computacionais, p. 347-356, 2008.

PMI – Project Management Institute. *A Guide to the Project Management Body of Knowledge, 4ed.* Newton Square: PMI Publications, 2008.

RATIONAL Software Corporation. *Rational unified Process, Version 2003.06.00.65, CD-ROM.* Rational Software Corporation, Cupertino, California, 2003.

ROCHA, P. Q. & BELCHIOR, A. D. *Mapeamento do Gerenciamento de Riscos no PMBOK, CMMI-SW e RUP.* VI Simpósio Internacional de Melhoria de Processos de Software, 2004.

SEI – Software Engineering Institute. *CMMI for Development (CMMI-DEV), Version 1.2, Technical Report CMU/SEI-2006-TR-008.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.

SEI – Software Engineering Institute. *Executive Overview of the SEI MOSAIC: Managing for Success Using a Risk-Based Approach. Technical Note CMU/SEI-2007-TN-008.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2007.