



# Gestão De Riscos De Processos De Negócio, Compliance E Controles Internos: Uma Agenda De Pesquisa

▶ Introdução .....	2
▶ Abordagem de Pesquisa .....	4
▶ Condução do Estudo .....	6
▶ Questões da Modelagem de Processos.....	9
▶ Desafios à Modelagem de Processos .....	12
▶ Discussão e Implicações .....	15
▶ Conclusões e Agenda de Pesquisa .....	18
▶ Referências Bibliográficas .....	19
▶ Apêndice .....	21
▶ Sobre o BPM360.....	22

## Artigo Principal

### Resumo

*A integração entre gestão de riscos e gestão de controles está se tornando uma área importante, desde o surgimento da Sarbanes-Oxley Act e o desenvolvimento de frameworks, como o Enterprise Risk Management (ERM) do Committee of Sponsoring Organizations of the Treadway Commission (COSO). Baseado em uma abordagem metodológica indutiva, a partir de uma revisão da literatura sobre o assunto e de entrevistas com gestores engajados em gestão de riscos e em projetos de controles internos, esse artigo identifica três áreas principais que atualmente têm uma atenção especial dos gestores. São elas: a gestão de riscos de processos de negócio, a gestão de compliance e o desenvolvimento de controles internos. Esse artigo discute essas questões e estabelece uma série de questionamentos considerando essas questões críticas.*

### Abstract

*Integration of risk management and management control is emerging as an important area in the wake of the Sarbanes-Oxley Act and with ongoing development of frameworks such as the Enterprise Risk Management (ERM) framework from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Based on an inductive methodological approach using literature review and interviews with managers engaged in risk management and internal control projects, this paper identifies three main areas that currently have management attention. These are business process risk management, compliance management and internal control development. This paper discusses these issues and identifies a series of research questions regarding these critical issues.*

## Introdução

Nós vivemos em um mundo incerto. Eventos que nós pensávamos que jamais aconteceriam aconteceram e eventos que nós pensávamos que aconteceriam não aconteceram. No esmaecer de colapsos financeiros, ataques terroristas, falhas em grandes sistemas de computadores e alertas sobre saúde, existe um grande foco em gestão de riscos - não somente como um aspecto específico das operações das companhias, mas como uma questão de integração empresarial, extrapolando seus limites geográficos e organizacionais.

A gestão de riscos é uma área relativamente madura de pesquisa em diversas funções operacionais tais como produção, logística, tecnologia da informação e saúde e segurança (Charette 1990; Borodzicz 2005). A teoria da tomada de decisão define risco como “variação reflexiva na distribuição de resultados possíveis, suas probabilidades e seus valores subjetivos” (March & Saphira 1987). O risco pode ser expresso matematicamente como “a probabilidade de ocorrência de perdas/ganhos multiplicado por sua respectiva magnitude” (Jaafari 2001).

A avaliação de risco envolve identificar ameaças e analisar a probabilidade dessas ameaças realmente ocorrerem. Gestão de riscos é gerir o que aconteceria se essas ameaças se materializassem, incluindo planos de recuperação de desastres, gestão de crises e procedimentos de emergência (Borodzicz 2005). Trata-se, também, de minimizar a probabilidade de ocorrência da ameaça levando a efeitos indesejados, através do desenvolvimento, implementação e operação de controles internos que mitigam, evitam ou transferem riscos (Ibid).

Talvez a definição mais reconhecida de controle interno é a do *Committe of Sponsoring Organizations of the Treadway Commission (COSO)* (COSO 1992; 2004), que o define como um processo, executado por diretores, gestores e outros quadros, projetados para proporcionar uma garantia razoável quanto ao atingimento dos objetivos, considerando: (i) a estratégia da empresa; (ii) eficácia e eficiência de operações; (iii) confiabilidade de relatórios financeiros; e (iv) *compliance*<sup>1</sup> com leis e regulações aplicáveis.

Esse artigo relata os resultados de uma pesquisa focada nas relações entre gestão de riscos e controles internos. Como esse é um campo de pesquisa emergente, esse artigo objetiva desenvolver um entendimento orientado à prática dos conceitos e questões envolvidas. Baseado em entrevistas com as profissionais e uma subsequente revisão da literatura, propõe-se uma agenda de pesquisa que pode guiar pesquisadores interessados nesse domínio que se desenvolve rapidamente.

A estrutura do artigo segue dessa forma: a próxima seção descreve a metodologia do projeto, a seção 3 apresenta os resultados, a seção 4 discute estes resultados e a seção 5 conclui o artigo com uma agenda de pesquisa proposta.

## 2 Metodologia

Baseado em uma abordagem de pesquisa indutiva, o objetivo desse projeto era esclarecer os problemas envolvidos e propor uma agenda de pesquisa orientada à realidade dos especialistas. Para esse propósito, uma abordagem de duas etapas foi escolhida:

1. Entrevistas iniciais, com os especialistas selecionados, com o objetivo de esclarecer a relação entre gestão de riscos e controles internos, bem como identificar seus problemas relevantes;

<sup>1</sup>Significa aderência a leis e regulamentações. Refere-se tanto ao alinhamento externo (leis de governo, órgão reguladores) quanto ao alinhamento interno (normas ISSO, códigos de conduta). (N. do T.)

2. A revisão da literatura subsequente para estudar qual pesquisa atual pode apoiar gestores organizacionais, considerando os problemas identificados durante as entrevistas, uma revisão da literatura focada em jornais acadêmicos, assim como em publicações voltadas para esse campo da pesquisa. Esse último foi incluído para a pesquisa de novas questões, as quais, comumente, aparecem nesses tipos de jornais, primeiramente.

Essas entrevistas foram feitas com cinco grandes empresas internacionais. Três dessas reuniões foram presenciais, enquanto dois desses encontros foram conferências por telefone. A seleção dessas companhias foi baseada, principalmente, em:

1. Percepção de relevância e grau de conscientização em relação às questões: as companhias deviam ter foco em gestão de riscos e controles internos. Esse foco poderia ser tanto em cima das operações quanto em cima dos serviços oferecidos (isto é, consultorias).
2. Tamanho: as companhias precisavam ter um tamanho mínimo para formalizar a gestão de riscos e controles internos como processos.
3. Acessibilidade: as companhias selecionadas eram baseadas na evidência prévia do seu apoio a pesquisas na área e nas suas relações com as instituições de pesquisa envolvidas.

As características das companhias entrevistadas são mostradas na tabela 1:

	Companhia 1	Companhia 2	Companhia 3	Companhia 4	Companhia 5
Indústria	Banco	Banco	Mineração	Consultoria/ Auditoria	Consultoria/ Auditoria
Turnover 2005 (em escala global)	13.8 bilhões de dólares australianos	11.3 bilhões de dólares	21.0 bilhões de dólares	29.3 bilhões de dólares	21.8 bilhões de dólares
Empregados <i>full time</i> 2005 (em escala global)	39.000	35.000	33.000	130.000	120.000
Gerente entrevistado	Gerente de Qualidade e Eficiência dos Negócios	Gerente de Riscos Operacionais	Gerente de Melhoria de Negócios	Gerente Sênior	Gerente Sênior

**Tabela 1 - As companhias entrevistadas**

Uma metodologia de entrevistas foi adotada utilizando um guia de entrevistas semi-estruturado listando várias questões gerais dentro da gestão de riscos e controles internos. No entanto, ele não foi seguido à risca, encorajando os gestores a falar o que normalmente prendia a atenção deles em relação à gestão de riscos e controles internos.

Nós sabemos das limitações empíricas da nossa abordagem. O propósito dessa abordagem é apontar áreas que normalmente têm maior atenção dos gestores e, dessa maneira, ajudam no foco da nossa busca por literaturas.

## Resultados

Nas entrevistas com esses cinco gestores, os problemas discutidos poderiam ser classificados dentro de três grandes áreas emergentes, baseadas em descrições dos “projetos em andamento” nas companhias ou baseadas em problemas que prendiam atenção dos gestores. São elas:

1. Gestão de riscos de processos de negócio;
2. *Compliance*;
3. Desenvolvimento de controles internos.

Elas são descritas abaixo, mostrando os problemas identificados em entrevistas, seguidas pelos resultados da revisão da literatura.

### 3.1 Gestão de Riscos de Processos de Negócio: As Entrevistas

Relacionar BPM com a gestão de riscos parecia ser de grande interesse por parte dos gestores. Eles descreveram vários problemas nesse campo:

1. Os gestores mencionaram diferenças na percepção dos riscos tanto a um nível organizacional quanto a um nível processual. No entanto, as implicações destas percepções para a gestão de riscos de processos de negócio não são tão claras. Além disso, o desdobramento conceitual da gestão de riscos de um processo de negócio (por exemplo, risco operacional, risco de TI, risco financeiro, risco de *compliance*, risco legal, risco de saúde e segurança etc.) diferencia-se entre funções e organizações, a qual poderia impactar na gestão de processos.
2. O risco precisa ser descrito de maneira consistente através dos vários níveis de arquiteturas de processos de negócio. Normalmente, não há um método ou ferramenta de modelagem usada para esse propósito. Um método para mapear e descrever riscos precisa ser integrado com linguagens de modelagem de processos de negócio.
3. À medida que as companhias vão se tornando mais globais em suas operações, com suas organizações mais distribuídas e conectadas a cadeias de suprimentos globais, o nível de

gestão e da análise de riscos está mudando. Há uma mudança de foco de riscos locais e regionais para riscos globais. Entender o impacto dessa mudança para processos de negócio é crucial.

4. A materialização do risco e os efeitos resultantes custam dinheiro, mas a gestão de riscos e controles internos também, ambos os casos gerando perdas reais e potenciais de efetividade e oportunidade. Os gestores se referem à importância de um entendimento de custos de riscos e de custos para mitigar esses riscos em uma perspectiva de processos de negócio, incluindo os custos de deixar o risco materializar-se versus os custos de controle para aquele risco.

### 3.2 Gestão de Riscos de Processos de Negócios: A Literatura

A área de BPM tem sido identificada como um das questões principais em gestão de negócios (Harmon 2003). O termo Business Process Management (ou BPM) refere-se a um conjunto de atividades as quais as organizações podem realizar, tanto para otimizar seus processos de negócio quanto para adaptá-los a novas necessidades organizacionais. Os processos de negócio de uma organização podem ser vistos como um local onde os riscos se materializam, onde a informação é gerada e usada e onde as atividades de controles são conduzidas.

Existe uma relação estreita entre processos de negócio e riscos. Por um lado, a gestão de riscos pode ser vista como um processo de negócio, isto é, diferentes estágios de um ciclo de vida de um risco formam processos de negócio, os quais requerem gestão. Por outro lado, o risco é um importante fenômeno de negócio, o qual deve ser considerado no (re)projeto de processos de negócio. Embora exista essa relação tão próxima, as comunidades de processos e gestão de riscos são grupos separados, com diferentes agendas de pesquisa e metodologias (zur Muellen & Rosemann 2005).

O propósito da gestão de riscos é “reduzir ou neutralizar riscos em potencial e simultaneamente oferecer oportunidades para melhorias sobre a sua performance.” (Ward & Chapman 1994, p.23). O *framework* geral de gestão de riscos é composto de três fases de ação principais: identificação, análise e controle (Kliem 2000). Os riscos são causados por várias incertezas. Logo, não é fácil modelar *frameworks* de riscos de uma maneira precisa. Uma maneira de fazer isso é caracterizar riscos usando propriedades como impacto, probabilidade, tempo de ocorrência e combinando-os com outros riscos (Gemmer 1997). Como riscos são comumente associados com resultados negativos (March et al. 1987), a distinção entre riscos e problemas, geralmente, não é muito clara. O risco não é necessariamente um problema, mas um “problema em potencial” que talvez seja resultado de uma tomada de decisão em particular (Charette 1990).

No contexto de BPM, o risco tem sido entendido como um fator em gestão de projetos relacionado a processos. Uma exceção é o estudo de caso realizado por Ballou (et al. 2000) Os autores discutem riscos a nível de processos de negócio, mas seus estudos sobre processos permanecem em um alto nível de abstração e o risco é tratado sob uma perspectiva financeira e geral de riscos de negócio, enquanto riscos operacionais, a nível de atividades, não são comentados.

Suh and Han (2003) propõem o uso de decomposição funcional e o Processo de Hierarquia Analítica para identificar negócios relacionados a riscos em infraestruturas de sistemas de informação (SI) de uma organização. Eles usam um modelo funcional de operações de negócios como uma diretriz para avaliar a criticidade de componentes individuais de IS. Essa visão tradicional de uma organização não é aplicável para componentes interfuncionais que podem apoiar funções de negócios múltiplas e ela não apóia a visão de operações de negócios orientada a processos.

Yu et al. (1999) discute diferentes modelos para estudar possíveis modos de falha, seus efeitos e suas criticidades. Ele lista o método *Risk Priority Number (RPN)* e um método de dimensionar os custos esperados como adequados para determinar riscos relacionados a processos. Baseado em procedimentos operacionais manuais, os autores apresentam uma técnica de análise crítica de falhas humanas que permite a verificação dessas possíveis falhas em um dado processo de negócio. Essa técnica de análise leva a uma árvore de erros e às suas probabilidades, mas não integra com outras técnicas de modelos conceituais.

Um *framework* sobre controles influente, que relaciona gestão de riscos com processos de negócio e com controles internos é o COBIT - particularmente, em sua versão mais recente (COBIT 4.0 in ITGI 2005) e na aplicação específica do framework para *compliance* com a *Sarbanes-Oxley* (ITGI 2004). O framework COBIT para gestão de riscos de *compliance* e de controles foca-se, especificamente, em aplicações de controles gerais e em larga escala que são relacionados a processos de negócio como manufatura, vendas e logística.

Isso indica, claramente, a demanda por modelos mais conceituais em relação aos princípios de gestão de processos de riscos. Existe uma necessidade para integrar o risco com arquiteturas de empresas estabelecidas, técnicas e ferramentas de modelagem de processos. Além disso, existe uma necessidade para desenvolver arquiteturas técnicas para riscos – isto é, a integração de todos os sistemas de gestão de riscos em uma única solução holística. Isso ainda não tem sido abordado na literatura.

### 3.3 Gestão de *Compliance*: As Entrevistas

Outra área que normalmente tem a atenção dos gestores é o *compliance*. Embora induzido por uma legislação alto-nível como o *Sarbanes-Oxley Act*, o *compliance* é uma área extensa e inclui cumprimento de leis e regulações de saúde e segurança, de meio ambiente, relativas ao trabalho e à proteção ao consumidor. Entretanto, os gestores entrevistados vêem isso sob uma perspectiva de gestão de riscos com foco em risco de não cumprimento das leis e regulações e estavam preocupados com a organização e com os controles necessários para garantir o *compliance*. As questões mencionadas foram:

1. O *compliance* é um processo de negócio e pode ser abordado como tal. Entretanto, abordá-lo dessa maneira ainda é algo prematuro e as diferenças entre diversos processos de *compliance* na organização (nos níveis locais, regionais e globais), bem como a integração entre eles, não são bem entendidos. Não existe qualquer modo geral de modelagem e descrição do processo de gestão de *compliance* e suas relações com modelos de processos de negócios.
2. Em particular, os gestores mencionaram alguns problemas com *compliance* global. Por exemplo, para uma companhia matriz operando nos Estados Unidos, os requisitos da *Sarbanes-Oxley* irão impactar em todas as entidades controladas por essa companhia. Outro exemplo é uma companhia que escolhe operar fábricas pelo mundo de acordo com o melhor padrão de prática ambiental do mundo. Esse tema complica ainda mais os problemas herdados em processos locais de *compliance* e agrega desafios a mais.
3. Não cumprir com legislações podem gerar prejuízos, como as multas. No entanto, isso pode gerar prejuízos também devido a danos à reputação da empresa, perda de confiança do consumidor ou perda de interesses do investidor. Medir esses custos pode ser importante, ao considerar, por exemplo, decisões sobre se deve-se operar em uma região ou não.
4. A gestão de *compliance*, no entanto, possui um ciclo de vida como todos os outros processos de gestão. Não existe, porém, um entendimento claro das fases da gestão de *compliance*, tais como etapas de não integração para integração total em processos de negócio, de manualidade para automatização, de local para global, de responsabilidade organizacional desagregada para *Chief Compliance Manager*, dentre outros. A estrutura

para prestação de contas de *compliance* foi mencionada como sendo algo importante, já que um crescente foco em *compliance* (à medida que as estruturas para gerar *compliance* ficam mais complexas) aumenta a necessidade de uma coordenação e de uma função de gestão na companhia.

### 3.4 Gestão de *Compliance*: A Literatura

Aparentemente, nos últimos dois anos, o *compliance* tem se tornado um chavão. Entretanto, companhias sempre tiveram que cumprir com leis e regulamentações, incluindo requisitos de saúde e segurança, de leis de impostos, de proteção ao consumidor e de leis trabalhistas.

Fatores que têm aumentado o foco atual em gestão de *compliance* são:

1. Extensos requisitos que vêm surgindo para se cumprir (como cumprimento com *Sarbanes-Oxley*), necessitando de *compliance* a níveis locais, regionais e globais em diferentes processos de negócios e, em alguns casos, de comprovação dos altos níveis de gestão ;
2. Custos com *compliance*. Um estudo da Fortune 1000 por Charles Rivers & Assoc. em 2005 mostrou que as companhias gastaram, em média, US\$ 5.9 milhões em *compliance* com requisitos da SOX em 2004 (CRA 2005). Um estudo similar do *AMR Research* conclui que custos com *compliance* podem crescer significativamente em 2005-2010 (IMJ, 2004). À medida que os custos crescem, gestores procuram maneiras de se aumentar a eficiência e a eficácia de processos de *compliance* ;
3. O não cumprimento de leis e regulamentações custam tempo e recursos, incluindo custos indiretos como prejuízos com danos à reputação e com processos contra a empresa. Especificamente, os riscos de reputação são importantes para aquelas companhias que dependem de confiança pública ou da venda de produtos de alto valor agregado para consumidores (Testa 2005, DrugResearcher 2004) ;
4. A integração de processos de negócio, de tecnologia da informação e de pessoas pelas fronteiras geográficas, temporais e organizacionais está levando para novos riscos de *compliance* que devem ser analisados. Um exemplo poderia ser as regulamentações

para transporte de produtos perigosos entre locais variados, que devem estar em *compliance* com cadeias de suprimentos globais ;

Esse desenvolvimento na área de *compliance* demanda uma gestão cada vez maior para fazer disso uma responsabilidade de uma função de gestão específica (isto é, o *Chief Compliance Officer*<sup>2</sup>). Isso pode levar também para o desenvolvimento ou aquisição de um sistema de informação específico de gestão de *compliance*.

A passagem da SOX nos Estados Unidos tem exercido grande influência sobre como as companhias vêem *compliance* (Baker et al. 2006). O objetivo fundamental da SOX é minimizar o risco de fraude e de declarações financeiras significativamente deturpadas. Companhias devem focar-se explicitamente em diferentes tipos de riscos (tais como o risco de informação falsa em relatórios anuais ou sonegação de fundos) e os controles internos relacionados a esses riscos. Gestores de altos níveis hierárquicos devem atestar, publicamente, a confiabilidade desses controles. Essa situação adiciona uma dimensão de *compliance* externo para o conceito de gestão de riscos e controles (ITGI 2004; COSO 2004; CFO 2005).

A gestão de riscos de *compliance* tem sido relacionada dentro de áreas separadas, como SOX, controles internos e *report*<sup>3</sup> financeiro (e.g. Waldman 2005; Shue 2004; Kendal 2004; Byington & Christensen 2005), *compliance* ambiental (Gangadharan 2006), saúde ocupacional e segurança (Ashford & Caldart 2001) e várias leis trabalhistas incluindo leis de discriminação, trabalho infantil e proteção aos trabalhadores (Adams 2003).

O *compliance* é uma característica geral dos negócios. Primeiramente, toda companhia deve estar cumprindo com alguma legislação. Em segundo lugar, é um processo composto por diferentes etapas, como visão geral de legislações, identificação de requisitos, avaliação de práticas, análise de riscos de não cumprimento com normas, designação de prestação de contas, gestão de projetos, estruturas para *report*, etc. Entretanto, parece não existir qualquer pesquisa com foco em integração de processos por funções, em desenvolvimento de processos de *compliance* padronizados ou em exploração de problemas com *compliance* em um contexto regional ou global ou em como gerir e melhorar o *compliance* sob uma perspectiva de processos de negócio.

<sup>2</sup>Responsável por garantir que a empresa e seus empregados estejam em conformidade com regulações internas e externas.

<sup>3</sup>Emissão de relatórios financeiros para *stakeholders*.

### 3.5 Desenvolvimento de Controles Internos: As Entrevistas

A terceira área é a de controles internos e como eles são desenvolvidos e integrados em gestão de riscos e *compliance*. Eles têm sido cada vez mais importantes nos últimos anos. As questões identificadas são:

1. Os controles internos têm sido parte do processo de gestão, focando-se na implementação da estratégia e no alcance de objetivos. Recentemente, eles têm surgido como as questões principais em gestão de riscos e gestão de *compliance*. Os controles são estabelecidos para mitigar riscos, os quais são inerentes a processos de negócio (isto é, o risco de fraude, o risco de erros de dados), e para assegurar *compliance* com legislação ou com objetivos de negócio. A integração entre processos de negócio, gestão de riscos e controles ainda não está bem avançada e é frequentemente aprendida através da prática nas companhias;
2. Os requisitos da Sarbanes-Oxley necessitam de melhorias substanciais para os controles internos. Durante muito tempo, eles parecem ter atravessado vários estágios de desenvolvimento. Esse desenvolvimento, as características de cada estágio e os fatores contingentes afetando cada estágio desse desenvolvimento não são bem entendidos mas são importantes, no sentido de que as companhias poderiam melhorar o seu desempenho tendo uma visão geral das forças e fraquezas em cada estágio ;
3. Os controles internos operam em vários níveis. Existem, por exemplo, controles comportamentais, controles de informação, controles operacionais, controles preventivos, controles capazes de detectar problemas, controles de aplicação e controles gerais. Os controles internos, no entanto, são dependentes de controles ambientais. Fatores de controle ambiental incluem integridade, valores éticos e competência de pessoas de entidades, filosofia de gestão e estilo de operação, a maneira como a gestão designa autoridade e responsabilidade, como a entidade organiza e desenvolve seu pessoal e a atenção e direção fornecida pelos gestores. Entretanto, a relação entre esses controles gerais da organização e atividades de controle individuais não são bem entendidas ;
4. Problemas específicos envolvendo o *compliance* com a *Sarbanes-Oxley* foram levantados pelos gerentes de auditoria entrevistados. Eles gostariam de saber mais sobre interpretações de companhias e firmas de auditoria sobre materialidade, fraquezas materiais, deficiências significantes e efetividade dos controles em um contexto sob a

SOX. Além disso, ao entender a divulgação com relação às fraquezas de controles internos em relatórios corporativos anuais, esses problemas vieram à tona.

Parece que os gestores entrevistados vêem essas três áreas de maneira intimamente interrelacionadas. Isso significa que esforços com *compliance*, gestão de riscos em processos de negócio e desenvolvimento de controles internos estão ligados a certas atividades específicas e comuns a mais de uma área. Exemplos mencionados foram *Sarbanes-Oxley*, a qual é um esforço de *compliance* que requer análises de riscos e desenvolvimento de controles internos. Outro exemplo mencionado é a eliminação de lixo nuclear, o qual requer extensos procedimentos de gestão de riscose, *compliance* com legislação e dependência de numerosos procedimentos de controles internos. Um terceiro exemplo é a detecção de fraude, a qual requer uma análise de riscos e um desenvolvimento de controles internos e afeta o *compliance* com legislação de *report* financeiro.

### 3.6 Desenvolvimento de Controles Internos: A Literatura

Uma revisão da literatura levanta a seguinte questão: existe uma diferença entre controles internos e gestão de controles? Existem diferentes definições (Rikhardsson et al. 2005), mas esses dois conceitos estão intimamente relacionados. Ambos estão focados na competência dos gestores para conduzir as organizações na direção especificada pela estratégia e pelos objetivos organizacionais, bem como identificar e reagir a mudanças internas e externas que talvez afetem esse curso. Uma definição muito usada para gestão de controles é “...as rotinas formais e baseadas em informações que gestores usam para manter ou alterar padrões em atividades organizacionais” (Simons 1995: p. 5). No entanto, a definição de controles internos da COSO (1992) também inclui *compliance* e *report* externo como objetivos de controle específicos, bem como de estratégia e operações. Além disso, controle interno, enquanto um conceito, é mais específico do que a mais acadêmica definição de gestão de controles.

A revisão da literatura relevante mostra que a evolução de um entendimento acadêmico de gestão de controles e controles internos já passou por, pelo menos, duas etapas evolucionárias nas últimas décadas. Essas etapas são vistas como complementares e não como resultantes de um entendimento mutuamente exclusivo de controles internos.

Da década de 1960 em diante, a gestão de controles é vista como um sistema de gestão cibernético, incluindo impulsos ambientais, respostas organizacionais e alcance de objetivos organizacionais. A gestão de controles é vista, principalmente, como um processo de informação em que gestores planejam, agem e reagem a impulsos externos e internos (e. g. Ittner & Larcker

2001; Otley & Berry 1980; Flamholtz et al. 1985). Na década de 1990, começa a surgir a visão de que a gestão de controles é um sistema ou processo focado em estratégia de implementação em um ambiente em que a estratégia precisa ser revisada sob uma base em andamento (e. g. Simons, 1995; 2000; Kaplan e Norton 1996, Chenhall 2003; Anthony & Govindarajan 2003; Merchant & Van der Stede 2003).

Uma revisão de uma literatura mais recente, entretanto, sugere que o entendimento prático e acadêmico está entrando em uma terceira fase em que o foco é mais em um conceito específico de controles internos. Essa fase vê os controles internos como um sistema objetivando estudar, minimizar e controlar riscos associados a processos de negócio de empresas, transações de negócio, aplicações de tecnologia de informação e disseminação de informação para tomadores de decisão internos e externos (e.g. ITGI 2004; COSO 2004; zur Mehlen & Rosemann 2005; Rikhardsson et. al. 2005).

Esse foco em riscos e gestão de riscos de controles internos é aparente em alguns *frameworks* influentes que têm sido publicados recentemente nesse campo. Um *framework* desse tipo é o *COSO Enterprise Risk Management (ERM)* (de 2004, mas iniciado em um *framework* anterior, da COSO, de 1992).

No *framework* da *COSO Enterprise Risk Management (ERM)*, ERM é definido da seguinte forma (COSO 2004, p. 2): “*Enterprise Risk Management* é um processo, efetuado pelos diretores, gestores e outros funcionários de uma empresa, aplicado para o estabelecimento da estratégia e para toda a empresa, projetado para identificar eventos em potencial que possam afetar a entidade, e gerir riscos para que ele esteja dentro do seu apetite, a fim de fornecer uma segurança razoável relacionada com o cumprimento dos objetivos da entidade”.

Diferentemente dos *frameworks* anteriores e das ferramentas desenvolvidas nas últimas duas etapas evolucionárias, *frameworks* de controles internos atuais e suas ferramentas estão surgindo como conectores entre gestão de riscos com controles internos. Eles podem ser classificados em *frameworks* gerais como COSO ERM (COSO 2004) e *frameworks* específicos ou estudos sob medida para vários contextos incluindo tecnologia da informação (Shue 2004; Cannon & Growe 2004; Hamaker & Hutton 2004; CFO 2005), *compliance* corporativo (CRA 2005, Stephens 2005; Markham & Hamerman 2005; Byington & Christenssen 2005; Waldman 2005; Matyjewicz & D’Arcangelo 2004) e BPM (Zur Muellen & Rosemann 2005).

Existem mais pesquisas sobre as relações entre gestão de riscos e controles internos. Entretanto, para a maioria dos casos, parece existir um foco em desenvolver *frameworks* e interpretar

desenvolvimentos institucionais. Existe uma grande necessidade de pesquisas em larga escala documentando similaridades e diferenças entre companhias, o que influencia o desenvolvimento de controles internos para dadas situações, assim como para as características da indústria. Existe, também, uma necessidade para estudos de caso documentando as práticas nas companhias e experiências com o objetivo de mais práticas serem desenvolvidas.

## Discussão

Geralmente, poucos estudos acadêmicos têm se focado explicitamente na integração de gestão de riscos, *compliance* e controles internos. Jornais voltados para a realidade desse campo de estudos (tais como *Accountancy*, *Internal Auditor* and *The Information System and Control Journal*) têm se concentrado nesses problemas por algum tempo.

A revisão da literatura mostra que riscos e controles internos em processos de negócio estão sendo integrados em muitos frameworks, tais como o modelo ERM da COSO (2004) e o COBIT do ITGI (2005). A integração de *compliance*, controles internos e análises de risco estão presentes na aplicação do *framework* da COBIT para *compliance* com a SOX em ITGI (2004).

1. Controle de comportamento, tais como uso de salvaguardas de recursos e ativos para que alguns objetivos sejam alcançados (estratégico, operacional, *report* e *compliance*);
2. Controle sobre a qualidade da informação que gestores usam na tomada de decisão (por exemplo, relacionados a uso de recursos) ou *report* a atores sociais externos (por exemplo, relacionados a *compliance*).

Dada a importância da informação e da tecnologia de informação para alcançar os objetivos da empresa (ITGI 2004), essa dimensão precisa ser incluída quando se for definir e pesquisar controles internos (Granlund & Mouritsen 2003, Sutton 2005). A perspectiva da gestão de riscos inerente ao COSO vê uma informação como crítica se a organização deseja atingir seus objetivos através da tomada de decisão em todos os níveis, assim como o *report* de informações de qualidade para atores sociais externos. A qualidade da informação para tomada de decisão interna e externa e os controles para se assegurar a qualidade dessa informação são cruciais se a companhia deseja atingir seus objetivos definidos no *framework* da COSO. Qualidade da informação não é um conceito de um objetivo mas inclui características do usuário da informação, além do contexto ser usado em acurácia, integridade, confiabilidade, temporalidade e acessibilidade da informação (Wang & Strong 1996). Outros frameworks que têm lidado com

qualidade da informação e sistemas de informação são SysTrust e WebTrust do American Institute for Certified Public Accountants (AICPA) (AICPA & CICA 2003).

A revisão da literatura e as entrevistas mostram a gestão de riscos de processos de negócio e controles internos sendo relacionados, geralmente, com tecnologia de informação e com sistemas de *Enterprise Source Planning (ERP)*, especificamente. Por exemplo, incluir sistemas ERP e sistemas de informação de prestação de contas em gestão de *compliance* é crucial, particularmente em relação ao *compliance* com *Sarbanes-Oxley Act*. O *PCAOB Auditing Standard*<sup>4</sup> declara que “a natureza e as características do uso de uma companhia de tecnologia de informação em seu sistema de informação afeta os controles internos de uma companhia em *reports* financeiros” (ITGI 2004: p. 12). Questões integrando gestão de riscos, *compliance* e controles internos, nesse contexto, incluem:

1. Integração entre análises de risco de controles, falhas intencionais e não intencionais em processos de negócios, levando a dados incorretos sendo incluídos no sistema;
2. Consideração da possibilidade de controles automatizados em sistemas ERP, substituindo ou implementando controles manuais;
3. Consideração de mais controles preventivos, substituindo ou implementando controles que possam detectar problemas;
4. Foco em documentação de controles como um ingrediente crucial em análise de controles;
5. Consideração do papel de auditores internos e externos, levando em conta, por exemplo, teste de controles.

Resumindo, a gestão de riscos em processos de negócio, controles internos e *compliance* estão intimamente relacionados. A gestão de riscos tem uma grande aplicabilidade para desenvolvimento, implementação e operação de controles para mitigar, evitar ou transferir riscos. Todos eles estão relacionados com a estratégia corporativa e objetivos corporativos (estratégicos, operacionais, de *report* e *compliance*). A gestão de riscos e controles internos estão alocados no contexto de processos de negócio e de ambientes de sistema de informação. Isso é visto na Figura 1.

<sup>4</sup>Responsáveis pela definição dos critérios de aplicação e auditoria da SOX.

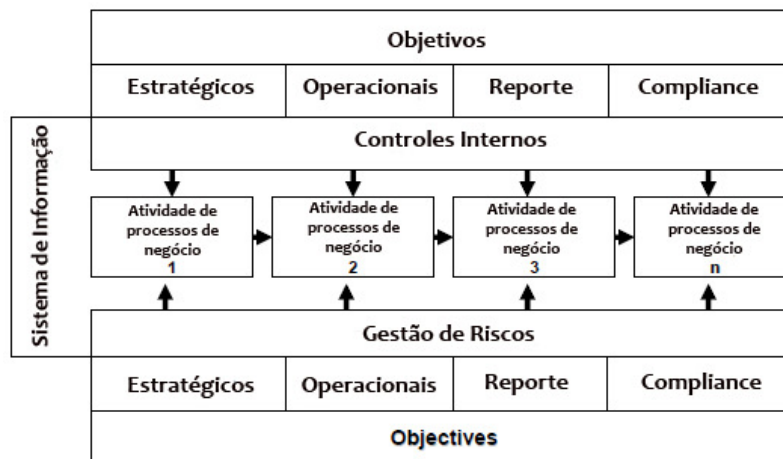


Figura 1 - Integração entre Gestão de Riscos, Compliance e Controles Internos no contexto de Processos de Negócio

## Conclusões e Agenda de Pesquisa

Da revisão da literatura e das entrevistas, é claro que a gestão de riscos, o *compliance* e os controles internos estão ficando mais integrados sob uma variedade de contextos de negócios.

Combinando e sintetizando a revisão da literatura e as entrevistas, nós introduzimos uma lista geral de perguntas que parecem relevantes para pesquisas mais aprofundadas na integração entre gestão de riscos e gestão de controles. As perguntas abaixo estão em um nível geral e precisariam ser especificadas sob as configurações de novas pesquisas em potencial.

### 5.1 Gestão de Riscos de Processos de Negócio

Existe uma necessidade de pesquisa dentro da área de modelagem de processos de risco relacionados a processos de negócios, pesquisando a padronização de gestão de riscos de processos de negócio e explorando o impacto de vários fatores de contingência em gestão de riscos de processos de negócio. Alguns questionamentos da pesquisa que precisam ser relacionadas são:

1. Como as companhias definem e conceituam riscos de processos de negócio e como eles selecionam controles para mitigarem esses riscos?
2. Como é um entendimento compartilhado dos riscos estratégicos, financeiros e de regulamentação principais para a organização?
3. Como os modelos de processos de negócio podem ser integrados com modelos de processos de controle?

4. Como um risco pode ser modelado para ele ser integrado a modelos de gestão de processos de negócio?
5. Como a eficiência e a efetividade de um sistema de gestão de riscos de processos de negócio são mensuradas?
6. Como o portfólio de riscos de uma empresa muda com a presença de controles automatizados?
7. Como os sistemas ERP incluídos em gestão de riscos em processos de negócio e quais controles são adotados?
8. Quais práticas de gestão de riscos estão estabelecidas considerando ameaças de danos à reputação e quais são os controles existentes?

## 5.2 Gestão de Riscos de Processos de *Compliance*

Existe uma necessidade de pesquisa em relação ao *compliance* a um nível mais agregado e não apenas com relação a cada função organizacional. Isso poderia implicar um foco geral nos processos gerais envolvendo *compliance*, em como esses processos atravessam fronteiras organizacionais e geográficas, assim como em explorar as influências do contexto em *compliance* e performance de *compliance*. Perguntas da pesquisa incluem:

1. Quais tipos de processos de *compliance* existem e como eles podem ser modelados?
2. Como a responsabilidade organizacional por *compliance* local, regional e global está evoluindo?
3. Como os problemas de *compliance* global estão sendo geridos nas empresas?
4. Quem são os vários interessados em performance de *compliance* e como as empresas lidam com isso?
5. Quais papéis e responsabilidades por requisitos de *compliance* existem nas companhias e quais práticas estão evoluindo?
6. Como um modelo de referência de processos de *compliance* seria?
7. Como podem as companhias desenvolver sistemas de alerta prévio para *compliance*?
8. Como podem os custos com não cumprimentos de legislações serem medidos?
9. O *compliance* liquida as altas cotações das ações da empresa?
10. Como as companhias usam TI para apoiar e consolidar o *compliance* e como a TI pode apoiar *compliance* mais efetivamente?

11. O *compliance* é mais efetivo em empresas com sistemas ERP do que em companhias sem sistemas ERP?

### 5.3 Desenvolvimento de Controles Internos

Existe uma longa tradição para a pesquisa em controles internos , especificamente no contexto de gestão de riscos e processos de negócio. Algumas perguntas que poderiam ser feitas:

1. Como os sistemas de controles internos estão evoluindo normalmente e quais estágios de maturidade de ciclos de vida eles atravessam?
2. Como as companhias interpretam o framework de controles da COSO no contexto da SOX? Existe um entendimento comum dos requisitos ou existem diferenças?
3. Como diferentes frameworks de controle se comparam, incluindo COSO, COBIT, WebTrust, SysTrust etc.?
4. Como as empresas estudam e desenvolvem controles internos na companhia como um todo?
5. Quais controles preventivos estão disponíveis para as companhias e como eles se diferem, considerando variáveis de contingente como tamanho, tecnologia, indústria e estrutura?
6. Como a eficiência e efetividade de um sistema de controle interno podem ser estudadas e comparadas, por exemplo, entre diferentes unidades de negócio?
7. Qual é o custo de eficiência de implementação de controles definidos pelo COBIT, comparado com os estudos de risco e efetividade de controles?
8. Os sistemas ERP significam práticas mais eficazes e eficientes de controles internos?

De uma forma geral, pode-se concluir que a intersecção entre gestão de riscos, BPM e *compliance* se dá muito mais pela necessidade de investigação e de pesquisa acadêmica (isto é, para o bem do entendimento de práticas organizacionais e institucionais), assim como uma pesquisa prática para contribuir com o desenvolvimento de soluções melhores, guias e frameworks para companhias.

## Referências Bibliográficas

1. Davies, I., Green, P., Rosemann, M., Indulska, M., Gallo, S.: How do Practitioners Use Conceptual Modeling in Practice? *Data & Knowledge Engineering* 58 (2006) 358-380
  2. Dumas, M., van der Aalst, W.M.P., ter Hofstede, A.H.M. (eds.): *Process Aware Information Systems: Bridging People and Software Through Process Technology*. John Wiley & Sons, Hoboken, New Jersey (2005)
  3. Davenport, T.H., Short, J.E.: The New Industrial Engineering: Information Technology and Business Process Redesign. *Sloan Management Review* 31 (1990) 11-27
- Adams, S. (2004). Age discrimination legislation and the employment of older workers. *Labour Economics*. Vol. 11 (2004): 219-241
- Ahrens, T. & C. S. Chapman (2004): Accounting for flexibility and efficiency: A field study of management control systems in a restaurant chain, *Contemporary Accounting Research*, volume 21, issue 2: 271-301 AICPA & CICA (2003). *Trust Services Principles and Criteria: Incorporating SysTrust and WebTrust*. American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Available from <http://www.webtrust.net/downloads/WT.TrustServices.pdf>. Accessed 3/5 2006.
- Anthony, R. & V. Govindarajan (2003). *Management Control Systems*. New York: MacGraw Hill.
- Ashford, N. & C. Caldart (2001). Negotiated environmental and occupational health and safety agreements in the United States: Lessons for policy. *Journal of Cleaner Production*. Vol. 9 (2001): 99-120.
- Baker R. W. E. Bealing Jr. D. A. Nelson A. Blair Staley (2006). An Institutional Perspective of the Sarbanes-Oxley Act. *Managerial Auditing Journal* 21(1): 23-33.
- Ballou, B., Godwin, N. H. and Tilbury, V. (2000) Riverfest: Managing Risk and Measuring Performance at Little Rock's Annual Music and Arts Festival. *Issues in Accounting Education*. Vol. 15: 483-512.
- Booker, S.; J. Gardner; L. Steelhammer; J. Zumbakvte (2004). What Is Your Risk Appetite? The Risk-IT Model. *International Information System and Control Journal*. Vol 2: pp. 5-9.
- Borodzicz, E. P. (2005). *Risk, Crisis and Management*. New York: John Wiley & Sons.
- Byington J. R. & J. A. Christensen (2005). SOX 404: How do you control your internal controls? *Journal of Corporate Accounting and Finance*. May/June 2005: 35-40.
- Cannon D. M. & G. A. Grove (2004). 'SOA Compliance: Will IT Sabotage your Efforts?' *Journal of Corporate Accounting & Finance*. July/August 2004: 31-37.
- Charette, R. (1990). *Applications Strategies for Risk Management*. McGraw-Hill New York.
- Chenhall, R. (2003). Management Control Systems Design Within its Organisational Context: Findings from Contingency-based research and Directions for the Future. *Accounting, Organizations and Society*. Vol.28 (2-3): 127-168.
- COSO - Committee of Sponsoring Organizations (COSO) (1992). *Internal Control - Integrated Framework*, [www.coso.org](http://www.coso.org). accessed February 26 2006
- COSO - Committee of Sponsoring Organizations (COSO) (2004). *Enterprise Risk Management*, [www.coso.org](http://www.coso.org). Accessed February 26 2006.
- CRA - Charles River & Associates (2005). *Sarbanes-Oxley Section 404: Costs and Remediation of Deficiencies: Estimates from a Sample of Fortune 1000 Companies*. Available from <http://www.crai.com>. Accessed 1/3 2006

Davenport, T. H., J. G. Harris & S. Cantrell (2004): Enterprise systems and ongoing process change, *Business Process Management Journal*, Vol.10 (1): 16-26.

DrugResearcher (2004) Non-compliance costs drug industry dear. <http://www.drugresearcher.com/news/ng.asp?id=54525-noncompliance-costs>. Accessed May 5 2006.

Emmanuel, C., D. Otley & K. Merchant (1995). *Accounting for Management Control*. London: Chapman & Hall.

Flamholtz, F. & T. K. Das (1985). Toward an Integrative Framework of Organizational Control. *Accounting Organizations and Society*. Vol 10(1): 35-50.

Gangadharan, L. (2006). Environmental compliance by firms in the manufacturing sector in Mexico. *Ecological Economics* – In Press 5/5 2006.

Gemmer, A. (1997). Risk Management: Moving Beyond Process. In *Computer*. Vol. 30: 33 - 43.

Granlund, M. & J. Mouritsen (2003). Introduction: problematizing the relationship between management control and information technology. *European Accounting Review*. Vol 12 (1): 77-83

Harmon, P. (2003). *Business Process Change*. Morgan Kaufman Publishers. San Francisco.

IMJ - Information Management Journal (2004). AMR Research 2004: Compliance Costs Are Rising. *Information Management Journal*. November/December: 6.

ITGI – IT Governance Institute (2004). *IT Control Objectives for Sarbanes-Oxley*. Rolling Meadows (IL): IT Governance Institute Available from [www.isaca.org](http://www.isaca.org). Accessed 1/3 2006.

ITGI – IT Governance Institute (2005). *Control Objectives for Information and related Technology*. Rolling Meadows (IL): IT Governance Institute. Available from [www.isaca.org](http://www.isaca.org). Accessed 1/3 2006.

Jaafari, A. (2001). Management of Risks, Uncertainties and Opportunities on Projects: Time for a Fundamental Shift. *International Journal of Project Management*. Vol. 19: 89-101.

Kendal K. (2004). A 10 Step Sarbanes-Oxley Solution. *Internal Auditor*. December 2004: pp. 51-55.

Kliem, R. L. (2000) Risk Management for Business Process Reengineering Projects, *Information Systems Management*. Vol. 17: 71-73.

March, J. G. & Z. Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science*, Vol. 33: 1404-1418.

Markham, R. & P. Hamerman (2005). *The Forrester Wave™: Sarbanes-Oxley Compliance Software*. Evaluation Of Top SOX Software Vendors Across 58 Criteria. Available from [www.forrester.com](http://www.forrester.com). Accessed May 3 2006

Matyjewicz G. & J. D'Arcangelo (2004). Beyond Sarbanes Oxley. *Internal Auditor* October 2004: 67-72.

Merchant, K. A. & Van der Stede, W. A. (2003). *Management Control Systems: Performance Measurement, Evaluation and Incentives*. London: Pearson/Prentice Hall.

Otley, D. & A. Berry (1980). Control, organization, and accounting. *Accounting, Organizations and Society*. Vol 5 (2): 231-246.

Rikhardsson, P. C. Rohde, A. Rom (2005). Exploring Enterprise Systems and Management Control in the Information Society: Developing a Conceptual Framework. Presented at the 6th International Research Symposium on Accounting Information Systems, December 10-11, 2005, Las Vegas, USA.

- Shue L. (2004). *Sarbanes Oxley and IT outsourcing*. Information System Audit and Control Association. Vol. 5: 5-9
- Simons, R. (1995). *Levers of Control*. Boston, Mass.: Harvard Business School Press.
- Simons, R. (2000). *Performance measurement and control systems for implementing strategy: Text & cases*, Upper Saddle River: PrenticeHall.
- Stephens, D. (2005). *The Sarbanes-Oxley Act: Record Management Implications*. *Records Management Journal*. Vol. 15(2): 98-103.
- Suh, B. and Han, I. (2003) *The IS Risk Analysis Based on a Business Model*. *Information & Management*, 41: 149-158.
- Sutton, S. (2005). *The Role of AIS in guiding Practice*. *International Journal of Accounting Information Systems*. Editorial. Vol 6. (2005): 1-4.
- Testa, B. (2005). *The high cost of noncompliance*. *Electronic Business Online* <http://www.reed-electronics.com/ebmag/article/CA6252379?pubdate=9%2F1%2F2005>. Accessed May 4 2006.
- Waldman, M. (2005). *Operationalizing Sarbanes-Oxley: How to Leverage Sarbanes-Oxley to Add Value to Business Operations*. Percipio Consulting Group. Available from <http://www.percipiogroup.com>. Accessed May 1 2006.
- Wang, R. & D. Strong (1996). *Beyond Accuracy: What Data Quality Means to Data Consumers*. *Journal of Management Information Systems*. Vol. 12 (4):5-34.
- Ward, S. and Chapman, C. (1994) *Transforming Project Risk Management into Project Uncertainty Management*. *International Journal of Project Management*. Vol. 21: 97-105.
- Yu, F.-J., Hwang, S.-L. and Huang, Y.-H. (1999) *Task Analysis for Industrial Work Process from Aspects of Human Reliability and System Safety*. *Risk Analysis*. Vol. 19: 401-415.
- zur Muehlen, M. & M. Rosemann (2005). *Integrating Risks in Business Process Models*. Presented at the 16th Australasian Conference on Information Systems, 29 Nov – 2 Dec 2005, Sydney.

## Sobre o BPM360

Visando difundir uma visão completa dos principais desafios existentes e tendências mundiais em BPM, a ELO Group e o Grupo de Produção Integrada da UFRJ estão lançando o portal BPM360.

Este portal traz uma série de publicações e comentários contendo as principais discussões existentes em torno do termo BPM ao redor do mundo. As publicações do BPM360 incluem: boas práticas internacionais, novos conceitos e idéias, dificuldades existentes com os métodos atuais de BPM, dentre muitos outros temas selecionados de forma criteriosa de acordo com seu grau de inovação, aplicabilidade prática e adequação ao contexto brasileiro.

Para trazer ao Brasil esta coletânea de publicações internacionais de referência em BPM, a ELO Group e o Grupo de Produção Integrada da UFRJ desenvolveram uma parceria com um dos maiores nomes da atualidade em BPM no mundo – o Professor Michael Rosemann. O Professor Rosemann é uma das principais referências internacionais em BPM, com publicações e trabalhos apresentados em 20 diferentes países, somente nos últimos três anos.

Ao longo dos próximos meses, diversos artigos contendo o que há de melhor no mundo de BPM serão traduzidos e disponibilizados neste portal de forma a disseminar para o Brasil as melhores práticas, conceitos e ferramentas em BPM.

---

"Nos últimos anos venho visitando diversos países e organizações e testemunhando diferentes abordagens e tendências na adoção de BPM. Desta forma, conforme surgiam novas experiências e aplicações em BPM, venho documentando estes novos desafios e iniciativas, consolidando-os em uma série de artigos desenvolvidos com parceiros, em sua maioria da *Queensland University of Technology*.

A proposta do BPM360 é realizar um giro de 360 graus nos diferentes conceitos, insights, ferramentas e abordagens relacionadas a BPM que vêm surgindo ao redor do mundo. Desta forma, uma seleção de artigos foi traduzida para o português e comentadas para promover discussões e reflexões a respeito do BPM em organizações, universidades e instituições brasileiras. É com grande prazer que compartilho estes artigos com você. Por favor sintam-se à vontade para nos contatar com contribuições, perguntas e comentários."

### **Prof. Michael Rosemann**

*Michael Rosemann é professor de Sistemas de Informações na Queensland University of Technology, onde é líder do Grupo de Pesquisa em BPM. Autor de cinco livros e 130 artigos, Michael Rosemann participou de cursos e conferências de BPM em mais de 20 países.*