2163-PS

COMPLIANCE CALIBRATOR'S ADHESION TO ELEMENTS OF INTERNAL CONTROL ACCORDING TO COSO: A CASE STUDY

Fabiana Lucas de Almeida (Universidade Federal de Minas Gerais, MG, Brasil) – fabialmeida83@hotmail.com
Rodney Pereira de Macedo (Universidade Federal de Minas Gerais, MG, Brasil) – orangebrazil@gmail.com

Abstract
Foreign companies that trade shares in the US market must present a certificate of internal control effectiveness in accordance with the Sarbanes Oxley Act (SOX). The Compliance Calibrator is one of the functionalities to comply with SOX requirements regarding segregation of duties. This paper uses a case study to investigate the deployment and use of the compliance calibrator as a tool for segregation duties in a Brazilian electricity sector company. The objective is to verify the Compliance Calibrator adherence with COSO methodology. Results show a straight adherence to COSO methodology in all of the five components COSO identifies as essential for effective internal control. There was also an increase in employees' perception about the consequences their actions in the company as a whole.

Keywords: Compliance Calibrator, SOX, COSO, Risk Matrix and Internal Control

A ADERÊNCIA DO *COMPLIANCE CALIBRATOR* AOS ELEMENTOS DE CONTROLE INTERNO DO COSO: UM ESTUDO DE CASO

Resumo
As empresas estrangeiras que negociam suas ações no mercado norte-americano devem apresentar certificação de eficácia de seus controles internos em consonância com a Lei *Sarbanes Oxley* (SOX). O *Compliance Calibrator* é uma das funcionalidades para atendimento às exigências da SOX relativas à segregação de funções. Este artigo utiliza um estudo de caso para investigar a implantação e a utilização do *Compliance Calibrator* como ferramenta de segregação de funções em uma empresa brasileira do setor e energia elétrica. O objetivo é verificar a aderência dessa ferramenta aos elementos de controle interno preconizados pelo COSO. Os resultados revelam robustez quanto à aderência à metodologia do COSO em seus cinco componentes essenciais para uma estrutura de controles internos efetivos. O estudo revela ainda que houve incremento na percepção dos funcionários sobre as conseqüências de suas ações para a empresa como um todo.

Palavras-chave: *Compliance Calibrator*, SOX, COSO, Matriz de Risco e Controle Interno

1. Introdução

Segundo as regras da *Securities and Exchange Commission* (SEC), as empresas estrangeiras que negociam suas ações no mercado norte-americano devem apresentar, juntamente com suas demonstrações contábeis consolidadas, a certificação de eficácia de controles internos em consonância com a Lei *Sarbanes Oxley* (SOX). Essa Lei tem a finalidade de proporcionar confiabilidade às Demonstrações Contábeis divulgadas no mercado financeiro, por meio da definição de uma estrutura de controles internos organizada e eficiente. A exigência da certificação para empresas brasileiras que negociam em bolsas de valores norte-americanas passou a vigorar em 2007, relativa ao exercício de 2006.

O *Public Companies Accounting Oversigth Board* (PCAOB), órgão privado sem fins lucrativos instituído pela Lei Sarbanes Oxley, estabelece que a avaliação da efetividade dos controles sobre os relatórios financeiros deve ser baseada em um padrão adequado e reconhecido, definido por um órgão de especialistas. Esse órgão recomenda a utilização do padrão de avaliação de controles internos definida pelo *Comitte of Sponsoring Organizations of the Treadway Comission* (COSO), órgão privado que tem como objetivo orientar as organizações nos aspectos relacionados à governança organizacional, ética de negócio, controles internos, gerenciamento de riscos corporativos, fraudes e reporte financeiro. A metodologia integrada do COSO identifica cinco componentes de controles essenciais para a efetividade dos controles internos: ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação, e monitoramento.

A adesão à Lei *Sarbanes Oxley* impactou de forma significativa o gerenciamento dos sistemas de informação das companhias. Para conformidade com os padrões estabelecidos pelo COSO, as companhias precisam assegurar que existem controles internos eficazes sobre as informações contábeis. Diante disso, são necessários procedimentos para manutenção da integridade das informações financeiras bem como políticas de segregação de funções e restrição de acesso a essas informações.

A segregação de funções para acesso a transações no sistema de informação é essencial para assegurar que as atividades de controle são eficazes na mitigação dos riscos relacionados a demonstrações contábeis. De acordo com a metodologia do COSO, as atividades são segregadas entre pessoas diferentes para reduzir o risco de erros ou ações inapropriadas. A base conceitual da segregação de funções está na definição de tarefas de forma que nenhum empregado esteja em posição de realizar fraudes ou incorrer em erros no curso normal de suas atividades. Por exemplo, as atividades de autorização e registro de transações, bem como a custódia dos ativos relacionados a essas transações devem ser segregadas a fim de evitar o uso inapropriado de recursos da companhia.

Uma das funcionalidades desenvolvidas pela *Virsa Systems,* para atendimento às exigências da Lei SOX, (daqui por diante denominada apenas SOX) relativas à segregação de funções, está totalmente integrada ao SAP/ERP. O *Virsa Compliance Calibrator* é direcionado aos controles do usuário e de acesso, incluindo o monitoramento de transações críticas em toda a extensão do sistema,

complementando o sistema de informações de auditoria e o gerenciamento dos recursos de controle interno.

De acordo com Pinar (2007) a implantação dessas soluções não pode assegurar uma abordagem de gerenciamento de risco sem mudar os procedimentos da organização. De fato, para Hunton (2002), a administração da companhia, bem como seus auditores internos e externos devem estar atentos ao surgimento de riscos diferentes em razão do sistema contábil, revisando suas estratégias contingenciais, controles internos e planos de auditoria.

Diante disso, e considerando que a utilização dessa ferramenta é recente no Brasil, o presente estudo tem como objetivo analisar, em uma situação prática, a aderência da funcionalidade *Virsa Compliance Calibrator* à metodologia do COSO, considerando seus cinco elementos de controle interno. Para tanto, analisou-se o conteúdo do *case* apresentado na Décima Conferência Anual da ASUG (*American SAP Users Group* – Associação de Usuários SAP), em 2007, sobre segregação de funções para adequação às exigências da SOX. O caso é referente à Companhia Energética de Minas Gerais (CEMIG), que em 2006 iniciou o projeto para implantação dessa ferramenta, com o intuito de certificar sua estrutura de controles internos em conformidade com a SOX. Os dados para análise de conteúdo foram também obtidos por meio de entrevista com um membro da auditoria interna de TI e um participante do projeto de implantação do sistema.

2. Referencial Teórico

2.1. Conformidades com a Lei Sarbanes Oxley e sistemas de informação

Em resposta aos escândalos corporativos ocorridos no início desta década, como o caso da Enron e da WordCom, o governo norte-americano implementou, em 2002, a Lei *Sarbanes Oxley* (SOX). O objetivo dessa lei é a proteção aos investidores a partir da implantação de uma estrutura de controles internos sobre a elaboração das demonstrações financeiras, garantindo maior acurácia e confiabilidade às informações. A regulamentação proporcionada pela SOX acerca da governança corporativa teve um impacto significativo no mundo dos negócios. Esta é aplicável, de forma geral, a empresas americanas e estrangeiras, bem como às suas subsidiárias, que negociam títulos no mercado americano.

A seção 404 da SOX exige a emissão, pela administração, de um relatório anual sobre os controles internos e procedimentos de emissão de relatórios financeiros, além de um certificado sobre a precisão do relatório dos auditores da empresa. A avaliação dos controles internos realizada pela administração deve ser baseada em procedimentos suficientes para avaliar o desenho e a eficácia operacional desses controles.

Para conformidade com a SOX, as companhias devem assegurar que suas transações financeiras são registradas de forma correta, válida e completa e que, dentre outras exigências, existe uma política de segregação de funções.

Para Rikhardsson, Best e Christensen (2006) a conformidade com a SOX envolve vários elementos, como a responsabilidade da administração e dos auditores externos, o reporte aos *stakeholders* e a qualidade dos dados. Esses autores acrescentam que uma questão chave para a SOX é o sistema de controles internos da companhia. Pinar (2007) afirma que os controles internos são desenhados para proporcionar razoável certeza de que os objetivos da

organização serão alcançados. Esses objetivos referem-se à efetividade e à eficiência das operações, confiabilidade dos relatórios financeiros e conformidade com as leis e regulamentos aplicáveis.

A Lei SOX não faz menção direta aos sistemas de informação. Entretanto, a estrutura de controles internos exigida para conformidade com essa Lei está intimamente ligada aos sistemas de informação, à medida que estes sustentam os registros das transações e das operações, além de serem responsáveis pelo fluxo interno e externo de informações.

Hauge (2007) afirma que a Lei *Sarbanes Oxley* é a principal responsável pela transformação do conceito de *compliance* em fator crucial do gerenciamento de sistemas para grandes organizações. Isso significa que a conformidade com a Lei *Sarbanes Oxley* impactou de forma significativa a estratégia de TI das organizações. Para Brown e Nasuti (2005) a metodologia adotada pela SOX deve estar alinhada à estratégia, à arquitetura e ao planejamento de processos para possibilitar o gerenciamento, a antecipação e a integração entre tecnologia e metodologia, visando assegurar um ambiente de TI estável e em contínuo desenvolvimento. Esse ambiente deve contribuir para a vantagem competitiva e estratégica da organização.

O PCAOB recomenda como padrão de avaliação de controles internos a utilização da metodologia do COSO. A aplicação de tal metodologia à tecnologia da informação está descrita na sessão seguinte.

2.2. A aplicação do COSO à tecnologia da informação

O COSO é um órgão privado sem fins lucrativos, fundado em 1985, com o objetivo de auxiliar as organizações na elaboração das informações financeiras de melhor qualidade, por meio da definição de uma metodologia dedicada à ética de negócios, aos controles internos efetivos e à governança corporativa. O COSO conta com a participação do *American Institute of Certified Public Accountants* (AICPA), do *American Accounting Association* (AAA), do *Financial Executives International* (FEI), do *Institute of Internal Auditors* (IIA) e do *Institute of Management Accountants* (IMA).

A tecnologia da informação representa um papel importante na operação estratégica dos sistemas de informação. Nos dias de hoje, tais sistemas são essenciais para proporcionar às organizações as habilidades necessárias para atender as demandas de seus clientes, fornecedores e demais *stakeholders*. Diante da importância da tecnologia da informação para os sistemas financeiros e operacionais, faz-se necessária a definição de uma estrutura de controles eficiente.

Para o IT Governance Institute (2006), o ambiente de controle de TI inclui o processo de governança de TI, o monitoramento e o reporte. O processo de governança de TI se refere ao plano estratégico de sistemas de informação, ao processo de gerenciamento de risco, ao gerenciamento de *compliance* e demandas regulatórias, e a políticas, procedimentos e padrões. A estrutura da governança de TI deve ser desenhada de forma que a tecnologia da informação agregue valor ao negócio e os riscos sejam mitigados. Deve também incluir uma estrutura organizacional que suporte uma adequada segregação de funções e leve a organização a atingir seus objetivos. Monitoramento e reporte são necessários para alinhar a tecnologia da informação às necessidades de negócio.

Para conformidade com a SOX, a tecnologia da informação deve estar alinhada aos componentes essenciais para uma estrutura de controles internos efetivos, definidos pela metodologia do COSO: ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação, e monitoramento.

O ambiente de controle se refere à cultura da organização que influencia a consciência de controle de seus funcionários. Funciona como fundação para todos os componentes de controle interno, proporcionando disciplina e estrutura. Os fatores do ambiente de controle são integridade, valores éticos, competência, filosofia da administração e estilo operacional. Ainda inclui a definição de autoridade e responsabilidade, organização e desenvolvimento de funcionários e a atenção e direção proporcionada pelo conselho de diretores.

O IT Governance Institute (2006) afirma que a tecnologia da informação possui características que requerem ênfase adicional no alinhamento dos negócios, responsabilidades, políticas e procedimentos e competência técnica. Além disso, a metodologia do COSO especifica que a definição de responsabilidades e a delegação de autoridades se relacionam aos objetivos da organização, às funções operacionais e aos requerimentos regulatórios, incluindo responsabilidade pelos sistemas de informação e autorização de mudanças.

A avaliação de risco é a identificação e a análise do conjunto de riscos relevantes para o alcance dos objetivos, formando a base para seu gerenciamento. Uma vez que ocorrerão mudanças constantes no ambiente econômico e regulatório e nas condições industriais e operacionais, são necessários mecanismos para identificar e gerenciar os riscos associados a essas mudanças. De fato, as organizações são envolvidas em vários riscos provenientes de fontes internas e externas que devem ser avaliados e mitigados. Para o IT Governance Institute, é provável que os riscos de controles internos possam ser mais pervasivos na organização de TI do que nas demais organizações da entidade.

Atividades de controle são políticas e procedimentos que garantem à administração que suas diretrizes são seguidas, ou seja, que as ações necessárias são adotadas para mitigar os riscos de os objetivos da organização não serem alcançados. As atividades de controle ocorrem em todos os níveis e funções da organização, incluindo aprovações, autorizações, verificações, reconciliações, revisões do desempenho das operações, segurança de ativos e segregação de funções.

O COSO divide os controles de sistemas de informação em duas categorias: controles de aplicação e controles gerais. Os controles gerais se aplicam a todos os sistemas de aplicação e auxiliam a garantir que estes operam adequadamente e de forma contínua. Os controles de aplicação incluem os passos computadorizados embutidos nos softwares de aplicação e demais procedimentos manuais necessários ao controle das transações. Uma vez integrados, esses controles garantem a totalidade, a acurácia e a validade das informações financeiras no sistema.

Os controles gerais são subdivididos nos seguintes tipos:

a) Controles de operações de Data Center: Controles como de configuração e programação de *jobs*, operação e *backup* de dados e planejamento contingencial de recuperação;
b) Controles de software de sistemas: Incluem os controles sobre aquisição, implantação e manutenção de softwares, gerenciamento da base de

dados, softwares de telecomunicações, softwares e utilidades de segurança.

c) Controle de segurança de acesso: Controles que protegem o sistema, prevenindo o acesso inapropriado e não autorizado. Tais controles restringem o acesso de usuários autorizados a funções necessárias a suas tarefas, suportando uma apropriada segregação de funções. O COSO acrescenta que o acesso de empregados antigos ou descontentes pode representar ameaças maiores para o sistema do que *hackers*.
d) Controles de manutenção e desenvolvimento de sistemas de aplicação: Representam os controles sobre a metodologia de desenvolvimento, incluindo desenho e implantação de sistemas, delineando fases específicas, documentação necessária, aprovações e checagem dos pontos, visando o controle do desenvolvimento e manutenção do projeto. A metodologia deve incluir controles sobre mudanças de sistema, que podem envolver autorização, aprovação, teste de resultados e protocolos de implantação.

Os controles de aplicação, como o próprio nome indica, são desenhados para controlar o processamento de aplicação.

Essas duas categorias de controles de sistemas de informação são inter-relacionadas, sendo os controles gerais necessários para garantir o funcionamento dos controles de aplicação que dependem de processamento computadorizado. Ambos são necessários para suportar o processamento da informação e a integridade da informação utilizada para gerenciar a organização.

O quarto componente do COSO, informação e comunicação, está voltado para identificação, captação e comunicação das informações pertinentes, no momento e formato necessário para capacitar as pessoas a executarem suas responsabilidades. A comunicação efetiva deve ocorrer em sentido amplo, fluindo do topo para o chão de fábrica da organização e vice e versa. Todos devem receber uma mensagem clara do topo da administração sobre as medidas de controle que devem ser tomadas, devendo estar conscientes de seu papel no sistema de controle interno e de como sua atividade individual se relaciona com o todo. Atenção deve ser dada também à efetividade da comunicação com as partes externas como clientes, fornecedores, reguladores e acionistas.

Segundo IT Governance Institute (2006), a identificação, o gerenciamento e a comunicação de informações relevantes representam um crescente desafio para o departamento de TI. A determinação de qual informação é requerida para atingir os objetivos de controle e a comunicação tempestiva dessa informação no formato necessário para proporcionar o desempenho das atividades individuais suportam esse elemento do COSO, que está intimamente ligado ao departamento de TI.

O COSO determina que os sistemas de controles internos devem ser monitorados. Esse monitoramento representa o quinto componente do COSO e consiste no processo de avaliação da qualidade do desempenho dos sistemas de controle interno. Este pode ocorrer através de atividades de monitoramento contínuo, avaliações separadas ou uma combinação de ambos.

Segundo IT Governance Institute (2006), a estrutura de controles internos sugerida pelo COSO para a conformidade com a SOX, como recomendado pela SEC, engloba os controles de tecnologia da informação, mas não determina objetivos de controle e atividades de controle relacionadas. Essas decisões

continuam a critério de cada organização. Conseqüentemente as organizações devem avaliar a natureza e a extensão dos controles de TI necessários para suportar seu programa de controles internos.

Brown e Nasuti (2005) afirmam que além do COSO, outras metodologias têm guiado as organizações no desenvolvimento do processo de TI. Estas buscam proporcionar melhores práticas e auxiliar na definição, na avaliação, no reporte e no desenvolvimento de controles internos nas organizações. Uma dessas metodologias é apresentada pelo *Control Objectives for Information and related Technology* (Cobit) que, de acordo com Brown e Nasuti, é considerada por muitos autores como o padrão de tecnologia da informação geralmente aceito para governança. O Cobit categoriza o processo de TI em quatro domínios: planejamento e organização, aquisição e implantação, distribuição e suporte e monitoramento. Além dos quatro domínios, o Cobit compreende 34 processos de TI e 215 objetivos de controle. Segundo IT Governance Institute (2006), o Cobit proporciona objetivos de controle e controles associados em nível de entidade e em nível de atividade, sendo largamente utilizado pelas organizações, como suplementar ao COSO.

Para o IT Governance Institute (2006), o processo de TI do Cobit tem relação com mais de um componente do COSO, dada a natureza dos controles gerais de TI, que sustentam a confiabilidade e a integridade dos controles de aplicação. Além disso, os controles de TI devem considerar toda a estrutura de governança para suportar a qualidade e a integridade da informação. Essa estrutura de governança de TI, por sua vez, deve proporcionar uma adequada segregação de funções.

2.3. O sistema *Compliance Calibrator*

Conforme metodologia do COSO, uma adequada política de segregação de funções é fundamental para a efetividade da estrutura de controles internos da organização. O conceito básico da segregação de funções está no reconhecimento de que empregados não devem estar em posição de cometer e dissimular fraudes ou erros no curso normal de suas atividades. As funções são segregadas entre diferentes funcionários para reduzir o risco de erro e de ações inapropriadas decorrentes de acesso a atividades que, em função de sua natureza, são conflitantes. A responsabilidade por registrar pagamentos e autorizá-los ou ainda o registro, a autorização e o manuseio de ativos são exemplos de tarefas conflitantes, do ponto de vista da avaliação do risco de fraudes, erros ou ações inapropriadas.

O sistema *Compliance Calibrator* é uma ferramenta disponibilizada pela *Virsa Sistems*, integrada ao SAP/R3, que auxilia na conformidade com a SOX através da análise de risco, detecção e remediação para controles de acesso ou autorização e segregação de funções. Tal sistema automatiza o controle de segregação de funções e de acesso a transações e permissões críticas, em conformidade com a seção 404 da SOX.

O sistema *Compliance Calibrator* permite, através do mapeamento e registro das atividades conflitantes, a mitigação dos riscos derivados da combinação destas. Quando um potencial risco ligado à segregação de funções é detectado pelo sistema, ele é reportado à pessoa responsável. Outra forma de ação do sistema é a simulação preventiva de potenciais violações, anteriormente à concessão de acesso ou autorização aos usuários.

De acordo com Hauge (2007), os auditores internos provavelmente irão propor a formalização de uma matriz de segregação de funções, se o projeto para mapeamento das transações conflitantes não o fizer. A matriz de segregação de funções descreve como segregar as tarefas entre os funcionários, como por exemplo, a compra e o recebimento de mercadorias ou a criação e a aprovação de documento de pagamento. Para proteger a organização de fraude e de roubo é necessário analisar o nível de risco para atividades como essas. Segundo Hauge (2007) existem tantos riscos de segregação de funções no sistema SAP que toda a biblioteca deste deve ser criada com o auxílio do sistema *Virsa Compliance Calibrator*.

Para entendimento do funcionamento do *Compliance Calibrator* é necessário conhecimento prévio da estrutura hierárquica de autorização do sistema SAP ERP. Para Pinar (2007), o SAP é hierarquicamente estruturado com os processos de negócio no topo, seguido pelas funções, pelas transações e pelos objetos. A figura 1 descreve a estrutura de autorização do sistema SAP.

Figura 1 – Estrutura de autorização do sistema SAP

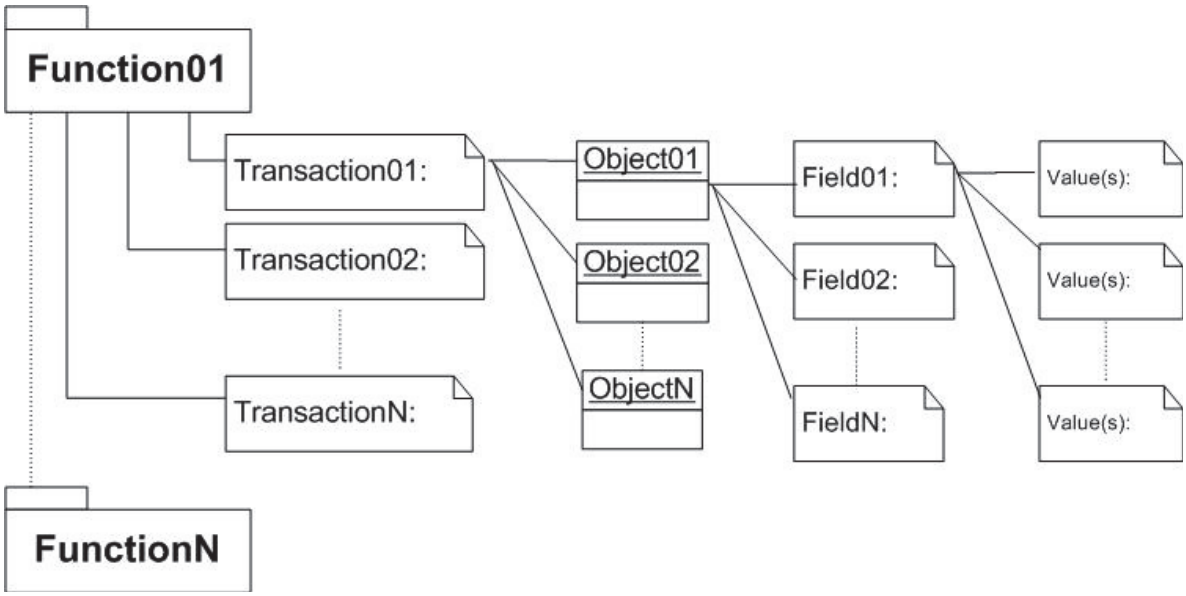

Figura 1: Estrutura de autorização do sistema SAP.
Fonte: Pinar (2007, p. 13)

Pinar (2007) afirma que as funções consistem em diferentes transações. Por outro lado, as transações podem estar em diferentes funções. Já os objetos pertencem a uma única transação, e os campos, por sua vez, pertencem a um objeto específico com seus valores. Dessa forma, o acesso dos usuários pode ser restrito em diferentes níveis, já que uma vez disponibilizados os direitos de uma transação, estes podem ser limitados em níveis inferiores, prevenindo a visualização de certos campos e impondo restrições aos possíveis valores que podem ser acessados naquele campo.

Hauge (2007) acrescenta que o sistema *Compliance Calibrator* é abrangente para o padrão de códigos de transações e objetos de autorização do SAP. Uma vez que o SAP adquiriu a companhia que desenvolveu esse sistema, Hauge

(2007) acredita existirem boas razões para crer que tal produto irá atingir um bom nível de confiança.

Segundo Pinar (2007), o sistema *Compliance Calibrator* executa as análises de segregação de funções em nível de transação e em nível de objeto. O COSO define que algumas funções devem ser segregadas a fim de prevenir fraudes, roubos e erros. Dessa forma, algumas transações não devem ser combinadas com outras e disponibilizadas ao mesmo usuário SAP. Pinar (2007) acrescenta que o sistema busca por conflitos resultantes da combinação de transações a partir de uma política de segregação de funções pré-definida, abrangendo as regras de negócio. A possibilidade de criação de regras em nível de objeto e valores ligados a ele restringe ou permite a um usuário executar transações em certas condições pré-definidas. Essa ferramenta do sistema possibilita a análise de risco em nível bem detalhado.

Segundo a SAP Brasil (2010), o sistema *Compliance Calibrator* está voltado para os controles de usuário e de acesso, incluindo o monitoramento de transações críticas em toda a extensão do sistema.

A SAP (2010) lista os seguintes benefícios principais do sistema *Compliance Calibrator*:

a) Verificação imediata e ampla da conformidade de autorizações do ERP;
b) Análise automática da segregação de funções e monitoramento de transações críticas;
c) Avaliação imediata dos riscos de autorização para os usuários, auditores e profissionais de segurança da área de TI;
d) Bloqueio das violações, antes que elas comprometam a produção;
e) Correções rápidas com verificação diária das causas que ocasionaram o problema;
f) Impossibilidade de análise manual e de falsos-positivos; e
g) Integração transparente com o SAP ERP, dispensando manutenção adicional de servidores ou dados.

Para Pinar (2007), o resultado da análise permite à administração verificar quais empregados possuem privilégios ou autorizações conflitantes. Além de estar em linha com as exigências da SOX, tal sistema é importante para garantir um ambiente de autorização mais seguro.

3. Procedimentos metodológicos

3.1. Delineamento da pesquisa

Selltiz *et al apud* Lakatos e Marconi (1990) classificam as pesquisas em estudos exploratórios, descritivos e de verificação de hipóteses causais. Os primeiros enfatizam a descoberta de idéias e discernimentos. Os estudos descritivos se caracterizam por descrever um fenômeno ou situação mediante um estudo realizado em determinado espaço-tempo. Os estudos de verificação de hipóteses causais englobam a explicação científica, e, em conseqüência, a sua previsão. De acordo com a taxonomia proposta por esses autores, a presente pesquisa se classifica como exploratória e descritiva. Exploratória porque existem poucos estudos sobre a aderência de um sistema de informação a um modelo teórico voltado para governança corporativa e porque investiga um assunto ainda pouco estudado. Segundo Gil (1989), as pesquisas exploratórias são construídas com objetivo de proporcionar visão geral de tipo aproximativo, acerca de

determinado fato. O estudo se caracteriza como descritivo, porque teve como objetivo descrever as características de um determinado fenômeno e estabelecer possíveis relações entre as variáveis.

Quanto ao método, esta pesquisa configura-se como um estudo de caso, tendo como objeto uma grande corporação do setor elétrico brasileiro, a Companhia Energética de Minas Gerais (CEMIG). De acordo com Yin (2005), o estudo de caso é uma investigação empírica que pesquisa um fenômeno contemporâneo dentro do seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos. Esse autor afirma que por meio do estudo de caso único podem-se obter análises mais detalhadas sobre a unidade em estudo e chegar a conclusões com maior nível de profundidade.

A CEMIG foi escolhida como unidade de estudo devido sua participação na Décima Conferência Anual da ASUG, em 2007, quando apresentou um *case* sobre segregação de funções para adequação às exigências da SOX. Ademais, houve disponibilidade de acesso aos dados dessa empresa. A CEMIG atua nas áreas de geração, transmissão e distribuição de energia elétrica e soluções energéticas, com ativos e negócios em dezoito estados brasileiros e no Distrito Federal, além do Chile. É uma empresa de economia mista de capital aberto, controlada pelo governo do estado de Minas Gerais e suas ações estão listadas nas bolsas de valores de São Paulo (Bovespa), Nova Iorque e Madri (Latibex). Encontra-se, há nove anos, no Índice Dow Jones de Sustentabilidade (CEMIG: 2009).

3.2. Coleta de dados

De acordo com Yin (2005), a informação pode assumir diversas formas e deve ser objeto de coleta de dados para o pesquisador. Nesta pesquisa foram utilizadas mais de uma fonte de dados, objetivando o desenvolvimento de linhas convergentes de investigação. Os dados foram coletados através do *case* apresentado na Décima Conferência Anual da ASUG e por meio de entrevistas com um auditor interno e com um técnico da área de tecnologia da informação, ambos participantes do projeto de implantação do sistema em análise. O roteiro das entrevistas foi elaborado com base na segunda edição do documento *IT Control Objectives for Sarbanes Oxley – The role of IT in the design and implementation of internal control over financial reporting*, elaborado pelo *IT Governance Institute*.

As entrevistas semi-estruturadas foram gravadas na própria empresa e posteriormente integralmente transcritas em papel, para facilitar a análise. Martins e Theóphilo (2007) afirmam que nesse tipo de entrevista utiliza-se um roteiro, mas há liberdade para se acrescentar novas questões. As entrevistas possibilitam a adição de elementos para corroborar evidências coletadas de outras fontes. No caso desta pesquisa, elas foram essenciais para confirmar o conteúdo do *case* apresentado na Décima Conferência anual da ASUG.

Para análise dos dados, utilizaram-se os procedimentos propostos por Bardin (1977), com relação às técnicas de análise de conteúdo. Essa autora define a análise de conteúdo como o conjunto de técnicas de análise das comunicações para tratamentos de dados que tem como objetivo identificar o que se diz a respeito de determinado assunto. Nesta pesquisa, seguiram-se as três etapas

propostas por Bardin: pré-análise, exploração do material e tratamento dos dados, inferência e interpretação.

Bardin (1977) apresenta três critérios de categorização para a análise de conteúdo: modelo aberto, modelo fechado e modelo misto. No modelo aberto, as categorias tomam forma no decorrer do processo de análise enquanto que no modelo fechado o pesquisador estabelece previamente as categorias com base em um modelo teórico. O modelo misto, por sua vez, faz uso dos dois modelos anteriores, estabelecendo inicialmente categorias que poderão ser modificadas no decorrer do processo de análise.

Optou-se pela utilização do modelo fechado de categorização, estabelecendo-se previamente as categorias com base no modelo teórico estudado (os cinco elementos da metodologia do COSO). Dessa forma, o conteúdo dos dados coletados foi analisado partindo do conceito teórico de cinco categorias: ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação, e monitoramento.

4. Análise dos dados

Preliminarmente à análise de dados é importante destacar que a empresa analisada passou por dois processos distintos de avaliação e de mapeamento de riscos na segregação de funções com utilização do *Compliance Calibrator*: O primeiro, em 2006, quando da implantação desta ferramenta; o segundo, em 2009, com a migração para a versão atual, incluindo o Sistema de Gestão de Consumidores (SGC), implantado efetivamente em 2008.

Em 2006 esse processo de avaliação de riscos ocorreu essencialmente em nível de transação. Embora a definição dos riscos tenha ocorrido em um nível superficial, este resultou em maior conservadorismo.

A versão implantada em 2009 envolveu a elaboração de uma estrutura de projeto no qual foram alocados dois funcionários da empresa analisada e quatro consultores externos para os trabalhos. O SAP já possui essa nova versão, denominada *Risk Analysis and Remediation (RAR)*. A análise dos dados expõe aspectos da experiência obtida com essas duas versões, apesar de o foco estar no *case* apresentado com base na primeira versão.

Para facilitar o entendimento, cada componente essencial a uma estrutura de controles internos efetivos, conforme metodologia do COSO, é analisado em tópicos distintos, de acordo com a categorização da análise de conteúdo realizada, com se segue.

4.1. Ambiente de Controle

O *Compliance Calibrator* não é integrado a nenhum outro sistema da empresa analisada que não esteja na plataforma SAP. Tal sistema está integrado ao R3 desde 2006, e está sendo implantado, em 2009, em outra ferramenta do sistema SAP denominada Sistema de Gestão de Consumidores (SGC). No caso da Cemig, a plataforma SAP envolve a maior parte das atividades da empresa. Na integração do *Compliance Calibrator* ao SGC, está sendo utilizada a nova versão desse sistema. Ressalta-se que, segundo os entrevistados, o *Compliance Calibrator* é configurado em nível de sistema e não de módulos. Dessa forma, ele se adéqua a qualquer módulo que esteja na plataforma SAP, bastando apenas configuração para tal. Esses fatos possibilitam a utilização do *Compliance*

Calibrator em um número cada vez maior de atividades da empresa, o que vai ao encontro das recomendações do IT Governance Institute (2006) de que os componentes técnicos de uma organização como um todo estejam integrados a um sistema de controle interno.

A empresa de consultoria externa *Opensis* e *Pricewaterhouse and Coopers* auxiliaram na condução dos trabalhos de implantação da primeira e segunda versões, respectivamente. Essas consultorias foram contratadas especialmente em função de sua *expertise* em assuntos relacionados à avaliação de riscos e controles para atendimento às exigências da SOX. Em 2009, elaborou-se a matriz de riscos para o SGC e realizou-se uma revisão de acessos a esse sistema. Os gestores da informação [1]foram responsáveis por revisar quais usuários estavam com riscos nas funções ou transações. O Grupo de Segurança da Informação (GSI) é responsável pela manutenção do sistema. Esse grupo é responsável por alterar as regras de segregação de funções cadastradas, além de informar a existência de risco e sua mitigação. A Auditoria Interna (AI) é responsável pela realização de testes periódicos de acordo com a metodologia pré-definida. Basicamente são três grupos com perfis específicos: gestores, GSI e AI. O sistema SGC segue a mesma linha. O trabalho integrado entre consultores externos e funcionários da empresa, além permitir o compartilhamento de experiências, está em conformidade com o COSO no sentido de terceirizar processos sobre os quais os recursos humanos da empresa não têm domínio técnico.

A etapa do projeto destinada à qualificação do pessoal envolvido na implantação, na manutenção e no monitoramento do *Compliance Calibrator* se estendeu por cinco meses, considerando a implantação da ferramenta nos ambientes de desenvolvimento, testes e produção. Na prática, isso aconteceu durante todo o projeto. Em uma sala específica para treinamento, todos os gestores foram treinados na extração de relatórios e orientados quanto aos riscos. Previamente, a equipe do projeto fez visitas e entrevistas pontuais com os gestores que participaram de todo o processo, desde o mapeamento das transações críticas até o treinamento final. A capacitação do GSI ocorreu no mesmo período de treinamento dos gestores da informação. Destaca-se que antes do *Compliance Calibrator*, o GSI efetuava a inclusão dos acessos, mas não realizada simulação de conflitos. O *Compliance Calibrator* representou uma mudança de cultura em relação à autorização, uma vez que para toda associação de novo perfil é feita a simulação.

As responsabilidades pelos controles internos relacionados ao *Compliance Calibrator* foram definidos pelo GSI e pela auditoria, com orientações da consultoria. A equipe do GSI, como responsável pela segurança da informação, tem a atribuição de identificar o perfil no qual uma transação está, sempre que houver solicitação de nova transação. A entrada desse perfil é simulada conjuntamente aos perfis existentes na chave e o *Compliance Calibrator* retorna o resultado, após checar na matriz de riscos previamente definida, a existência de transações conflitantes dentro desse perfil de acesso[2]. Havendo o risco, solicita-se ao gestor da informação responsável pelo perfil a atenuação do risco. Dessa

[1] Gerente, ou empregado formalmente designado, responsável pelas informações e recursos sob sua gestão.

[2] Conjunto de autorizações/permissões de acesso que, atribuídas a um usuário de informática, permitem que ele exerça suas atividades profissionais nos sistemas informatizados da Empresa.

forma, o GSI verifica se o usuário realmente pode acessar a transação, consultando a área daquele usuário para constatação da real necessidade do acesso e da existência de aceitação daquele risco para aquele usuário. Caso aceite o risco, faz-se o cadastramento da atenuação no sistema *Compliance Calibrator* e associa-se o risco a um gestor. A cada três meses, esse gestor executa o monitoramento.

A empresa estudada utiliza o SAP desde 1999 e desde então já existia segregação de funções. O que efetivamente houve a partir do *Compliance Calibrator* foi maior segregação. Havia perfis com excesso de transações ou transações consideradas conflitantes do ponto de vista da avaliação de riscos realizada para conformidade com a SOX. Houve ainda aumento no número de perfis, resultante do desmembramento daqueles existentes. As exigências da SOX relacionadas à segregação de funções no sistema SAP foram apresentadas aos gestores, bem como as conseqüências da inobservância dessas exigências. A partir do momento que foi demonstrado ao gestor a sua responsabilidade diante o processo de segregação de funções, seu envolvimento no projeto cresceu.

4.2. Avaliação de Risco

A avaliação de risco preconizada pelo COSO para aplicação à tecnologia da informação versa sobre o risco de mudanças em ambiente regulatório e econômico. Como ferramenta de gestão e segregação exclusiva da plataforma SAP, essas mudanças não afetariam a utilização do *Compliance Calibrator* pela empresa analisada. A Cemig também não incorreu em risco de desenvolvimento porque o *Compliance Calibrator* é um sistema padrão. Poderia haver alguma customização[3], que não foi o caso, tanto em 2006, quanto para a versão atual. Contudo, houve riscos de implantação, que foram devidamente mapeados.

Não há, no departamento de TI, um grupo formado especificamente para certificar quais são os riscos ligados a TI para certificação SOX. Existem os controles SOX que foram criados paralelamente ao projeto de implantação do *Compliance Calibrator*.

O Departamento de Tecnologia da Informação (TI) disponibiliza um funcionário que acompanha todo o processo SOX, sendo ele o ponto de contato, tanto do auditor interno quanto do auditor externo. Esse funcionário não faz avaliação dos sistemas existentes na empresa, apenas coordena o trabalho relacionado à SOX. Existe ainda o grupo de qualidade de SOX, na área de desenvolvimento de sistemas, que analisa a adequação dos novos sistemas e dos sistemas já existentes às exigências da SOX. Esse grupo define regras de TI para desenvolvimento de sistemas, à luz do que está no Cobit, conforme determinado pela Auditoria Interna (AI), com base na SOX. A Auditoria interna é responsável pela gestão da certificação SOX, pois apóia os gestores responsáveis pelos controles nos desenhos, no plano de ação, além de realizar testes e verificar se os controles foram executados. Destaca-se que a existência e o trabalho do grupo de qualidade SOX condizem com as orientações do COSO de que as empresas devem ter uma subcomissão de planejamento de TI com o objetivo de avaliar a integridade de seus sistemas com as exigências da SOX.

Por outro lado, a Cemig não disponibiliza tratamento especial ou plano estratégico para controles internos relacionados ao *Compliance Calibrator*. Há

[3] Essa expressão não existe na língua portuguesa, mas é utilizada na empresa no sentido de adapatação

uma matriz com os controles e com a identificação dos responsáveis por esses controles. Qualquer funcionário que esteja nessa matriz é co-responsável pela certificação. Os controles de *Compliance Calibrator* existentes na matriz de controles da SOX são aqueles de revisão dos riscos, executados pelos gestores das áreas.

Na implantação do *Compliance Calibrator*, a avaliação formal de riscos, recomendada pelo COSO, foi uma etapa do projeto. Os gestores foram convidados a identificar as transações conflitantes e a definir os perfis. Os gerentes identificaram formalmente quem eram os usuários chaves de suas respectivas áreas (Finanças, Materiais, Projetos, Recursos Humanos, etc.). Com base nessa avaliação e no padrão de melhores práticas, as informações foram inseridas no *Compliance Calibrator*.

Para infra-estrutura de operações e de mudança, não existe plano de contingência. Como no caso do SGC o sistema *Compliance Calibrator* está na fase de implantação, sendo este o ponto de partida para o processo de segregação de funções neste sistema, não há um plano ou previsão de retorno. Normalmente quando se faz a implantação do sistema, esses planos estão vinculados ao retorno a uma situação inicial ou a uma situação anterior, o que não é o caso do SGC.

Para o SAP/R3, os planos de contingência para infra-estrutura de operações e mudanças nos processos *Compliance Calibrator* estão restritos à utilização de *backup*, que seria um controle geral, classificado como atividade de controle. Como o sistema dispõe de três ambientes (desenvolvimento, qualidade e produção), foi elaborado um procedimento para situações problemáticas no ambiente de produção, quando o ambiente de qualidade é transferido para a produção. Para evitar essas situações, todas as modificações no *Compliance Calibrator*, sobre customização no banco de dados, através de habilitação ou desabilitação de transações críticas[4] são feitas no ambiente de desenvolvimento e teste, passando posteriormente para o ambiente de produção. As simulações são no ambiente de produção quando da inclusão de uma transação de direito de acesso. Ressalta-se que, segundo um dos entrevistados, o *backup* é padrão dentro de TI e inclusive já foi necessário utilizá-lo para o *Compliance Calibrator*. A utilização de *backup* demonstra forte aderência às recomendações do Coso para controles gerais de sistemas de informação. Da mesma forma, a utilização de outro ambiente como plano contingencial já foi utilizado com sucesso. Contudo, não há normas formalizando a necessidade de se recorrer ao *backup* em caso de problemas, mas todos os funcionários já conhecem esse procedimento.

Os riscos identificados foram classificados, com auxilio dos gestores e da consultoria externa, em “riscos aceitáveis” e “não aceitáveis”. Eles foram segregados em graus de criticidade dos processos com base em práticas de mercado e suas aplicações à realidade da empresa, conforme Quadro I. O material sobre avaliação de risco, identificação de gestores, matriz de risco, etc. está arquivado e inclui alguns rascunhos, que estão no “arquivo morto” da empresa e em uma pasta informatizada. A elaboração da matriz de risco para segregação de funções com o auxílio do *Compliance Calibrator* converge ao entendimento de Hauge (2007). A documentação referente à definição de

[4] A Cemig considera uma transação crítica quando sua utilização inadequada causar riscos de interferência nos números do balanço, prejuízos financeiros, impactos nos negócios e repercussões negativas à sua imagem.

transações, nomeação de gestores, documentação de aceitação de risco está de posse da Auditoria Interna. Quando o gestor da informação necessita de uma transação nova no sistema, ele é questionado sobre o grau de criticidade dessa transação, por meio de um formulário no Outlook, que após preenchido, é remetido ao GSI.

Quadro I: Níveis e conseqüência dos riscos

Nível de Risco	Conseqüência	Nível de aprovação
Baixo	Possibilita perda de produtividade	Gerência responsável pelo processo, com ciência de sua respectiva superintendência. Esta terá o direito de veto da aprovação em questão.
Médio	Possibilita interrupção de processos	
Alto	Possibilita perda física ou financeira	Superintendência responsável pelo processo, com ciência de sua respectiva Diretoria. Esta terá o direito de veto da aprovação em questão.
Crítico	Possibilita perda física ou financeira relacionada a empregados com nível gerencial	Diretoria responsável pelo processo.

Fonte: Elaborado pelos autores, com base no Case Cemig (2006)

O acúmulo de funções ainda acontece em casos raros, apesar de a segregação ser o objetivo de se ter um sistema automatizado para gestão de funções. Há situações, por exemplo, em que apenas um funcionário trabalha em localidade distante ou mesmo em uma pequena usina de geração de energia. Dessa forma, para dar agilidade ao processo, o acúmulo pode ser permitido, com o devido controle por parte do gerente e a devida atenuação do risco, o que não está em desacordo com a metodologia do COSO. Como é grande o número de usuários do SAP na empresa (aproximadamente 1830 em 2006), dificilmente se consegue fazer gestão dos conflitos sem uma ferramenta automatizada. A categorização de conflitos em níveis requer que cada nível de risco tenha uma alçada competente para aprovação, conforme Quadro I. Até novembro de 2009, ninguém havia submetido ao diretor a aceitação de um risco crítico. Em 2006, quando o *Compliance Calibrator* foi implantado no R3, existia usuário com acesso para criar e aprovar pedido de compra (acesso às duas transações). Durante o projeto houve entendimento que essas transações eram críticas e que deveriam estar segregadas. Com a implantação do sistema *Compliance Calibrator*, não existe usuário com acesso para criação e aprovação de pedido de compra simultaneamente. Para o SGC, deve-se seguir essa mesma linha de raciocínio, ou seja, atividades conflitantes, como criação e baixa de fatura, deverão ser segregadas.

4.3. Atividades de controle

Quando do desenvolvimento ou mudanças de sistemas, deve-se alterar a documentação que define objetivos, funcionalidades, especificações técnicas, planos de teste, etc. Na Cemig, deve-se atender ao processo de documento de

software da TI. No caso do *Compliance Calibrator* não houve necessidade dessas alterações, uma vez que tal sistema é fechado e suas funcionalidades são bastante abrangentes. Mas caso ocorressem situações que justificassem alguma alteração, os procedimentos próprios existentes para documentação de softwares de TI teriam sido seguidos.

Em termos de implantação, a empresa analisada mapeou controles sobre o desenho destacando fases específicas, documentação requerida, mudanças no gerenciamento, aprovação e pontos de inspeção para controlar o desenvolvimento ou manutenção do projeto. Alguns gerentes optaram pela carga de perfis a serem controlados por um determinado gestor dentro de uma área.

Desde a implantação do *Compliance Calibrator*, quando se cria um perfil novo, solicita-se ao gerente enviar à Auditoria Interna, conforme um normativo interno (I10, anexo 3), a formalização do gestor da informação.

O *Compliance Calibrator* possibilita a avaliação do risco de acesso a transações conflitantes por um mesmo usuário por meio da simulação, quando da inclusão de novos acessos. Um usuário para o qual haja risco somente é cadastrado no sistema se houver a aceitação desse risco pelo responsável, de acordo com alçada competente definida em instrução de informática. Adicionalmente, o gestor da informação periodicamente, executa o relatório de risco para verificação da existência de usuário associado a um risco. Caso seja identificado usuário associado a um risco, o gestor deve verificar se este já está atenuado Esse monitoramento é feito no ambiente de produção, pois o usuário final só existe no ambiente produtivo.

O COSO preconiza atenção aos riscos com usuários antigos ou descontentes, pois eles seriam mais ameaçadores que hackers. Nesse sentido, os funcionários que se desligam da empresa perdem imediatamente o acesso a qualquer transação no SAP. O problema com os descontentes é minimizado pelo conhecimento dos gerentes sobre o histórico de trabalho de seus subordinados usuários do sistema. Esse tipo de problema não ocorreu tanto antes quanto depois da implantação do *compliance calibrator*.

A geração do relatório de risco pelos gestores da informação é a atividade requerida para manutenção do funcionamento do sistema, de forma a obter sucesso no processo de segregação das funções. No controle de acesso, os gestores da informação fazem a extração do relatório de risco a cada noventa dias. Esse procedimento representa um controle SOX definido na matriz de riscos e controles da Auditoria Interna, que por sua vez, executa testes sobre esse procedimento, de acordo com a metodologia de auditoria adotada.

Para definir o que é conflitante, a matriz de risco *standard* apresentada pela SAP foi adaptada, sendo removidas e incluídas situações específicas em função da realidade de uma empresa de venda de energia. A partir daí, define-se quais transações não podem estar associadas às demais. São analisadas apenas transações de conflito da função, e não outros conflitos, como por exemplo, de grau de parentesco.

Não existem controles de aplicação[5] para o software dentro dos programas. As transações devem estar mapeadas dentro de um perfil, conforme definições de cada usuário, e as funções são criadas dentro do *Compliance Calibrator*. Esses

[5] Controles de aplicação são aqueles embutidos nos programas para prevenir transações não autorizadas.

controles são recomendados pelo COSO, mas não se aplicam à ferramenta *Compliance Calibrator*.

4.4. Informação e Comunicação

A informação dos riscos de acesso indevido gerada pelo *Compliance Calibrator* é oportuna e apropriada, conforme recomenda o COSO. O fluxo de informação gerada pelo *Compliance Calibrator* basicamente é do departamento de TI para o usuário final. Quando um risco previamente mapeado é identificado a partir da simulação, este departamento aciona o gestor da informação e informa que há um risco. Enquanto o risco não for mitigado ou atenuado, não há liberação de acesso para aquele usuário. Caso seja constatada necessidade de acesso pelo usuário em análise das transações em conflito, o gestor da informação deve aceitar o risco. Essa atenuação é feita mediante preenchimento de formulário de risco, elaborado a partir de ferramenta do Outlook.

Conforme os entrevistados, os riscos e as funções foram mapeados, segregados e definidos adequadamente. Não há registros de reclamações dos usuários a respeito do processo de informação e de comunicação e esse fato pode ser considerado positivo como *feedback* às recomendações do COSO. Apesar de não haver prazo formalmente estipulado, em no máximo dois dias as ações necessárias em razão de riscos identificados pelo *Compliance Calibrator* são solucionadas. O tempo de resposta não foi considerado um marco importante quando da elaboração do projeto.

Os controles para garantir que a informação gerada está correta são automáticos. Não há controles manuais. Também são automáticos os controles para garantir a restrição de acesso às informações geradas, e todos são cadastrados no *Compliance Calibrator*. Qualquer nova informação que passa pelo fluxo torna-se informação oficial. Tudo fica registrado em formulário eletrônico que funciona inclusive como medida para economizar papel. A ferramenta de rastreabilidade utilizada pela auditoria para tentar identificar o que gerou a mudança também é informatizada. A automatização e a informatização minimizam a possibilidade de falhas e de manipulação da informação.

Todos os indivíduos responsáveis por alguma atividade no sistema possuem acesso às informações, quando necessário. Todos eles acessam seus controles e relatórios respectivos para que vejam as atenuações pertinentes aos perfis e aos usuários determinados por ele.

As políticas e procedimentos sobre o *Compliance Calibrator* foram comunicados aos usuários por meio de ampla divulgação. Posteriormente houve o treinamento dos envolvidos no processo. Esse processo está sendo repetido com a implantação da nova versão, porém de maneira mais discreta, em função do trabalho já realizado quando da criação dos perfis do SGC. Em 2006, os gestores não tinham o conceito de controle de acesso. Atualmente, ao se criar os perfis, há participação da auditoria interna, que orienta os gestores da importância de se usar a ferramenta *Compliance Calibrator*. Ademais, a participação dos usuários em todas as fases do processo de implantação por si só, foi considerada um fator de mitigação de riscos de comunicação.

4.5. Monitoramento

O *Compliance Calibrator* permite tanto o monitoramento periódico quanto o monitoramento contínuo para mitigação dos riscos de segregação de função. A

versão antiga, implantada em 2006, não permite a emissão de alerta quando da violação de algum acesso. A versão atual, por sua vez, permite a emissão desse alerta ao gestor da informação, quando se realiza uma autorização. Dessa forma, a qualquer momento o gestor pode verificar quais são os riscos associados às suas funções e qual usuário está com risco. A auditoria interna também possui acesso à emissão do relatório de riscos.

Adicionalmente, existe controle SOX mapeado na matriz de riscos e controles da auditoria interna, relativo à geração, pelos gestores da informação, do relatório de riscos do *Compliance Calibrator*. Esse controle é testado pela auditoria interna periodicamente, de acordo com metodologia pré-definida. Todos esses procedimentos de monitoramento estão em conformidade com as proposições da metodologia do COSO, recomendada pelo PCAOB.

5. Conclusão

O *Compliance Calibrator* é uma moderna ferramenta para segregação de funções, com grande potencial de auxilio em controles internos, especialmente para empresas com grande número de usuários em seus diversos sistemas informatizados (Finanças, Recursos Humanos, Gestão de Clientes, Gestão de Materiais, etc.). Essa ferramenta é para uso exclusivo da plataforma SAP e pode ser utilizada para certificação de conformidade à Lei *Sarbanes Oxley*, o que a torna bastante útil para empresas que negociam ações nas bolsas de valores americanas, como é o caso da Cemig.

O estudo de caso realizado nesta empresa revelou que seu processo de segregação de funções utilizando o *Compliance Calibrator* apresenta robustez quanto à aderência à metodologia do COSO em seus cinco componentes essenciais a uma estrutura de controles internos efetivos: Ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação e monitoramento. A empresa estudada elabora matriz de risco, conforme defendido por Hauge (2007), em nível bem detalhado com o auxilio do *Compliance Calibrator*, conforme sugerido por Pinar (2007).

A ausência de formalização de alguns processos durante a implantação do *Compliance Calibrator*, a permanência do acúmulo de funções em casos especiais e a ausência de plano de contingência para infra-estrutura de operações e mudanças na implantação do SGC não podem ser considerados como desconformidades à metodologia do COSO, uma vez que, nas três situações, os riscos foram aceitos e mitigados, conforme cada caso.

Varias áreas da empresa foram impactadas com a implantação do *Compliance Calibrator.* Além de propiciar maior segurança na segregação de funções e de atender à conformidade com a SOX, os entrevistados destacaram como ponto positivo desse impacto, o incremento na percepção dos funcionários, especialmente dos gerentes, da responsabilidade e das conseqüências de suas ações para a empresa como um todo.

Os resultados desta pesquisa abrangem apenas uma empresa, de um setor específico da economia, o que impossibilita a aplicação de seus resultados a outras empresas. O sucesso com a implantação do *Compliance Calibrator* na empresa analisada pode não se repetir em outros estudos. Ressalta-se ainda, que esta pesquisa foi realizada considerando os cinco elementos de controle

interno da metodologia do COSO e o conteúdo do *case* apresentado pela Cemig na Décima Conferência Anual da ASUG.

A utilização dessa ferramenta é recente no Brasil: no setor de energia elétrica a Cemig foi pioneira. Dessa forma, recomenda-se aos interessados no tema, realizar estudos em empresas de atividades diferentes, considerando situações diferentes, como empresas que não se obrigam às exigências da SOX.

6. Referências bibliográficas

BARDIN, L. *Análise de Conteúdo*. Tradução: Luís Antero Reto e Augusto Pinheiro. Lisboa: Edições 70, 1995.

BROWN, W.; NASUTI, F. What ERP Systems can tell us about Sarbanes Oxley? Information Management & Computer Security. *Emerald Group Publisching*, [S.l.], 2005. Disponível em: <http://www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=B4D98D7E18594D210276BA7D5E4F47DD?contentType=Article&hdAction=lnkhtml&contentId=1513514>. Acesso em: 15 jan. 2010.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE THEADWAY COMMISSION- COSO. *Report: Framework. Chapters 2 - 6*, COSO, 1999. Disponível em: <www.coso.org>. Acesso em 15 jan. 2010.

COMPANHIA ENERGÉTICA DE MINAS GERAIS – CEMIG. *Quem Somos*. Disponível em: <http://www.cemig.com.br/>. Acesso em 15 jan. 2010.

CONFERÊNCIA ANUAL DA AMERICAN SAP USERS GROUP - ASUG, 10, 2007. *SAP Brasil. CEMIG Projeto segregação de funções – Segregação de função adequação SOX*, 2007. Disponível em: <http://www.sap.com/brazil/about/eventos/asug.epx>. Acesso em: 05 jun. 2009.

GIL, A. C. *Como elaborar projetos de pesquisa*. 2ª, São Paulo: Atlas, 1989.

HAUGE, O. C. *Application Based IDS Reporting in the ERP system SAP R/3.* Tese (Mestrado em ciência em segurança da informação) - Faculty of Computer Science and Media Technology. Gjovik: Gjovik University College, 2007. Disponível em: < http://www.accessroles.com/hauge-ids-in-sapr3.pdf>. Acesso em 15 jan. 2010.

HUNTON, J. E. Blending information and communication technology with accounting research. *Acconting Horizonts*, [S.l], n. 1, p. 55-67, 2002. Disponível em: <http://www.questia.com/googleScholar.qst?docId=5002464090>. Acesso em 15 jan. 2010.

IT Control Objectives for Sarbanes Oxley – The role of IT in the design and implementation of internal control over financial reporting. *IT Governance Institute*. Rolling Meadows, 2ª, 2006. Disponível em: < http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=12383>. Acesso em: 15 jun. 2010.

LAKATOS, E. M.; MARCONI, M. A. *Técnicas de Pesquisa*. 2ª; São Paulo: Atlas, 1990.

MARTINS, G. A.; THEÓPHILO, C. R. *Metodologia da Investigação Científica para Ciências Sociais Aplicadas*. São Paulo: Atlas, 2007.

PINAR, K. *Risk assessment of two sox compliance tools*. Techcische Universiteit Eindhoven. Departament of Mathematics and Computer Science, 2007. Disponível em < http://alexandria.tue.nl/extra1/afstversl/wsk-i/pinar2007.pdf>. Acesso em 15 jun. 09.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD – PCAOB. *Standards and Related Rules*: Standard 5 e Standard 2. PCAOB, 2007. Disponível em: <http://www.pcaob.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.5.aspx> Acesso em: 15 jun. 2009.

RICKHARDSSON, P; BEST., P.; JUHL-CHRISTENSEN, C. *Sarbanes Oxley compliance, internal control and ERP systems: Automation and the case of mySAP ERP*. Accounting Research Group, Working Papers A, 2006. Disponível em: < http://www.hha.dk/afl/wp/arg/A_2006_02.pdf>. Acesso em: 15 jan. 2010.

SAP. *SAP Compliance Calibrator by Virsa Systems*. SAP, 2009. Disponível em: <http://www.sap.com/netherlands/solutions/businesssuite/erp/financials/pdf/brochures/BWP_Compliance_Calibrator.pdf>. Acesso em 22 jul. 2009.

U.S. SECURITY AND EXCHANGE COMISSION – SEC. *Sarbanes Oxley Act. United States*, SEC, 2002. Disponível em: <www.sec.gov>. Acesso 15 jun. 2009.

YIN, R. K. *Estudo de caso: planejamento e métodos*. Tradução: Daniel Grassi. 3ª, Porto Alegre: Bookman, 2005.