A importância da Segurança da Informação e dos Controles Internos na Prevenção de Riscos à Estabilidade Financeira de uma Instituição Bancária

The Importance of the Security in Information and Internal Controls to Prevent any Risks to the Financial Stability at a Financial Institution

Juline Schneider
Canoas – RS
Guaduada em Ciências Contábeis pela UFRGS[1]
julinesch@hotmail.com

Ângela Rozane Leal de Souza
Porto Alegre – RS
Doutora em Agronegócios pela UFRGS
Mestre em Contabilidade pela UNISINOS[2]
Professora da UFRGS
angela.souza@ufrgs.br

Resumo

Em virtude das exigências mercadológicas crescentes, as instituições financeiras têm buscado melhorias em seus processos de Tecnologia da Informação (TI) e controles internos da Governança de TI –, especialmente aos voltados à minimização dos riscos de mercado, de liquidez e operacionais. Neste cenário, questiona-se o nível de conformidade da segurança da informação e dos controles internos para a prevenção de tais riscos em uma instituição financeira. Assim sendo, o presente estudo tem por objetivo comparar as práticas da segurança da informação e dos controles internos preceituados pela literatura especializada com a realidade de uma instituição financeira, visando à prevenção de riscos, por meio da análise das políticas internas da instituição. Para atingir esse objetivo, efetua-se um estudo de caso, com procedimentos de natureza documental, qualitativa e descritiva. Os principais resultados revelam que a instituição estudada tem uma organização adequada e em fase de crescimento, proporcional às suas finalidades comerciais. Entretanto, a mesma não se encontra inteiramente de acordo com o modelo COBIT, visto que este não é um instrumento obrigatório, mas apenas aconselhável às instituições financeiras pelo BACEN. E a empresa ainda se preocupa em manter um bom nível de eficácia e eficiência das operações, confiabilidade dos relatórios financeiros e cumprimento de leis e regulamentos aplicáveis. O gerenciamento dos riscos é efetuado segundo as definições do COSO, analisando então cada tipo de risco inerente ao ramo. Sob esse enfoque, a empresa determina diretrizes para os três tipos de riscos analisados, cada um com sua complexidade e peculiaridade.
Palavras-chave: Controle interno. Segurança de TI. Gestão de Riscos.

Abstract

As market demands are growing, so financial institutions seek to improve upon the process of Information Technology (IT) and internal control via the governance of IT, especially those that aim to reduce the risks in liquid and operational markets. In this scenario it is asked: what is the level of security necessary to keep the financial institution safe from all those risks? This study's purpose is to compare the vulnerability of information and internal controls within the reality of a financial institution, with the goal to prevent risks by analysis of the internal policies of said institution. To achieve this goal a case study is performed using three kinds of proceedings: documentary, qualitative and descriptive. The main results show that the studied institution has adequate organization and lives a growth phase, proportional to its commercial purposes. It is worth noting that the institution is not entirely in accordance with the COBIT model; however, that is not a required directive, only advice given to financial institutions by the Central Bank. In spite of this, the company cares about maintaining a good level of effectiveness and efficiency of operations, and maintaining the reliability of financial reporting and compliance within the applicable laws and regulations. Risk management is carried out according to the COSO settings, analyzing each type of risk in the business. Under this approach the company establishes guidelines for the three types of risk analyzed, each one with its complexity and uniqueness.
Keywords: Internal control. Governance of IT. Risk Management.

[1] UFRGS - Universidade Federal do Rio Grande do Sul – Porto Alegre – RS – CEP 90040-060.
[2] ` UNISINOS - Universidade do Vale do Rio dos Sinos - São Leopoldo - RS, CEP. 93022-750.

Artigo recebido: 09/05/2017 e aceito: 21/07/2017

1. Introdução

Recentemente, a Tecnologia da Informação (TI) tem se tornado fundamental aos negócios, de tal maneira que é praticamente impossível para muitas organizações sobreviverem e prosperarem sem o seu auxílio. Observa-se, conjuntamente, uma mudança na competição mercadológica, que está cada vez maior, o que exige muito mais da segurança das informações das empresas, bem como maior controle e gerenciamento dos seus riscos.

Desde os primórdios, o ser humano tem a necessidade de informação – seja ela visual, escrita, falada ou até mesmo pensada – para poder se comunicar, cooperar e evoluir. Sendo assim, pode-se dizer que a informação é a coleta, processamento e organização de dados. Entretanto, para as empresas de nada vale ter informações se não for possível garantir sua confidencialidade.

Um estudo sobre as práticas da segurança informacional, dos controles internos e riscos de uma instituição financeira pode ver visto como um meio de comprovar a sua importância para as organizações no mercado, cumprindo um dos princípios contábeis, a continuidade. Segundo o Conselho Federal de Contabilidade (CFC, 1993), "esse princípio pressupõe que a entidade continuará em operação no futuro", ou seja, o controle na empresa pode lhe assegurar a perpetuação no mercado. Assim, a questão problema que motiva essa pesquisa é: qual é o nível de conformidade da segurança da informação e dos controles internos para a prevenção de riscos em uma instituição financeira?

Desse modo, o objetivo deste estudo é comparar as práticas da segurança da informação e dos controles internos preceituados pela literatura especializada com a realidade da empresa estudada com vistas à prevenção de riscos.

2. Revisão de Literatura

2.1 O Modelo COBIT

O uso do modelo é aconselhável a empresas que aplicam a Governança de TI. "Do inglês *Control Objectives for Information and Related Technology* (COBIT), tal modelo é um guia formulado como *framework*, dirigido para a gestão de Tecnologia da Informação (TI)" (ASSI, 2012, p.133). O COBIT foi criado pelo *IT Governance Institute* e é recomendado pela ISACA (*Information Systems Audit and Control Foundation*), pois o mesmo tem diversos recursos que auxiliam a gestão da TI, como sumário executivo, controle de objetivos e mapas de auditoria, entre outros (ASSI, 2012).

Tuttle e Vandervelde (2007) afirmam que o COBIT foi originalmente destinado a ser utilizado pela administração de uma organização como uma ferramenta de *benchmarking*, composto pelas melhores práticas relacionadas aos controles de TI. Desde então e por causa de sua forte ênfase no controle, tanto os auditores internos como os externos o aplicam para auditorias de demonstrações financeiras, bem como auditorias operacionais e de conformidade.

As altas hierarquias das organizações estão percebendo crescentemente que, com mais informações e com segurança, as chances de sucesso tornam-se maiores. "Um modelo de controle da governança de TI define as razões pelas quais a governança de TI é necessária; quais são as partes interessadas e o que esse modelo precisa atingir" (ITGI, 2007, p.13).

Segundo Neves (2007) e Luciano (2010), o COBIT tem mecanismos de acompanhamento (relatórios e revisões por estágios) e a aprovação das fases subsequentes deve ser baseada na revisão e aceitação das entregas das fases prévias. Sua missão é pesquisar, desenvolver, publicar e promover um conjunto atualizado de objetivos de controle geralmente aceitos e aplicáveis a TI para uso de profissionais (ASSI, 2012).

Os processos de TI no COBIT são agrupados em quatro domínios (ITGI, 2007):

> a) Planejar e Organizar (PO): preocupa-se com a identificação sobre o que TI pode melhorar para atingir os objetivos de negócios;
>
> b) Adquirir e Implementar (AL): para executar a estratégia de TI, as soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, implementadas e integradas ao processo de negócios;
>
> c) Entregar e Apoiar (DS): trata da entrega dos serviços solicitados, o que inclui a própria entrega de serviço, gerenciamento da segurança e continuidade, serviços de apoio aos usuários e gerenciamento de dados e recursos operacionais;
>
> d) Monitorar e Avaliar (ME): aborda o gerenciamento de *performance*, o monitoramento do controle interno, a aderência regulatória e a governança.

Como caracteriza o ITGI (2007, p.19), "o modelo de maturidade para o gerenciamento e controle dos processos de TI é baseado num método de avaliar a organização, permitindo que esta seja pontuada de um nível de maturidade não existente (0) a otimizado (5)". Tais níveis são evidenciados no Quadro 1, a seguir:

Quadro 1: Modelo de Maturidade Genérico nos processos de TI

0) Inexistente	Completa falta de um processo reconhecido. A empresa nem mesmo reconheceu que existe uma questão a ser trabalhada.
1) Inicial/Ad hoc	Existem evidências de que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado; ao contrário, existem enfoques *ad hoc* que tendem a ser aplicados individualmente. O enfoque geral de gerenciamento é desorganizado.
2) Repetível, porém intuitivo	Os processos evoluíram para um estágio em que procedimentos similares são seguidos por diferentes pessoas que fazem a mesma tarefa. Não existe um treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixada com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e, consequentemente, erros podem ocorrer.
3) Processo definido	Procedimentos foram padronizados, documentados e comunicados por meio de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serão detectados. Os procedimentos não são sofisticados, mas existe a formalização das práticas existentes.
4) Gerenciado e mensurável	A gerência monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão sob constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.
5) Otimizado	Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade, como em outras organizações. TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e a efetividade, tornando a organização rápida em adaptar-se.

Fonte: Adaptado pelos autores, a partir de ITGI (2007).

Visualiza-se, no Quadro 1, um modelo genérico de como cada nível de maturidade pode ser descrito. No COBIT, uma definição genérica é provida para as escalas de maturidade deste código, as quais são similares às do CMM (*Capability Maturity Model*), mas interpretadas de acordo com a natureza dos processos de gerenciamento de TI do COBIT" (ITGI, 2007).

Já no que se refere à definição do termo "risco", este abarca a reflexão acerca da possibilidade de algo dar errado, ou incerteza, ou outras conceituações que remetam a uma situação desfavorável. Sobre a origem da palavra, cabe saber que é proveniente do latim risicu ou riscu, que significa "ousar" (IBGC, 2007; 2010). A partir do conceito anterior, pode-se concluir que o risco é qualquer evento que possa afetar os objetivos das organizações, conforme evidencia Filgueiras (2010, p. 401):

> "Torna-se muito complexo definir o que é risco, pois há inúmeros enfoques distintos de acordo com o contexto envolvido. Pode-se citar o risco de um acidente aéreo, quando envolve uma companhia seguradora; o risco de não conseguir uma marca olímpica, quando tratamos de um atleta qualquer, ou o risco de um grande prejuízo num negócio, quando o cenário é uma empresa."

Sobre outro enfoque, pode-se analisar o risco como oportunidade, pois o risco pode propiciar retorno positivo quando bem administrado, conforme evidencia Damodaran (2009), ao afirmar que o risco oferece oportunidades ao mesmo tempo em que nos expõe a resultados talvez indesejáveis. Ainda, Trapp e

Corrar (2005) definem risco como um evento, esperado ou não, que pode causar impacto no capital ou nos ganhos de uma instituição.

No que se refere à gestão de riscos, o Comitê de Supervisão Bancária da Basileia, no seu material *Princípios Fundamentais para uma Supervisão Bancária Efetiva* (2006), considera que a inadequada avaliação de riscos contribuiu decisivamente para os problemas de controles internos de algumas organizações bancárias e às perdas relacionadas.

Grazziotin (2002) ainda afirma que "os negócios bancários são arriscados pela sua própria natureza. Entretanto, conhecer os riscos tempestivamente e com a maior precisão possível é um dos pilares de um sistema de controles internos eficiente", permitindo uma pronta ação no sentido de evitá-los ou minimizá-los.

No mesmo sentido, Antunes (2004, p. 4) complementa:

> "...o resultado da avaliação dos riscos dos sistemas de controles internos de uma entidade é componente significativo no processo de determinação da natureza, época e extensão dos testes de auditoria por serem aplicados pelo autor independente de demonstrações contábeis."

Assim, os riscos são classificados de acordo com a atividade da empresa, sendo que, no presente trabalho, serão abordados os riscos de liquidez, de mercado, de crédito e operacionais. A classificação da natureza do risco permite sua agregação de uma forma organizada e de acordo com a sua natureza, em função das áreas da organização que são afetadas pelos eventos (IBGC, 2007, p. 18). Em outras palavras, é necessário conhecer a empresa em que será desenvolvida atividade de identificação de riscos, pois nem sempre um risco de uma empresa será igual para outra, em virtude do segmento, atuação, dentre outras peculiaridades. De maneira geral, avalia-se o risco de liquidez, de mercado e operacional, como segue.

a) Risco de liquidez

Fortuna (2008) define os riscos de liquidez como:

> "a ocorrência de desequilíbrios entre ativos negociados e passivos exigíveis e, portanto, descasamentos entre pagamentos e recebimentos, que possam afetar a capacidade de pagamento da instituição, levando-se em conta as diferentes moedas e prazos de liquidação de seus direitos e obrigações."

O Banco Central do Brasil (BACEN), na resolução 2.682/99, afirma que os riscos é que determinarão quanto as instituições financeiras terão que provisionar de suas operações de crédito.

b) Risco de mercado

No que se refere ao risco de mercado, este pode ser considerado como o evento que, possivelmente, acarretará perdas à empresa, decorrentes de movimentos inesperados no mercado atuante. Para evidenciar, Nascimento e Alves (2007, p. 3) propõem que riscos de mercado estão ligados a variações nos preços de mercado de ativos, passivos e demais instrumentos financeiros. Ainda, Caouett, Altman e Naryanan (2009, p. 3) acrescentam que é a chance de que o valor de um investimento se altere como resultado de forças de mercado, tais como taxas de juros, preços de *commodities* e níveis de moeda corrente. Do ponto de vista de Filgueiras (2010, p. 402), o risco de mercado:

> "representa o que podemos ganhar ou perder quando compramos ou vendemos um determinado ativo, contrato ou derivativo, pela simples mudança em seu preço. O risco de mercado está intimamente ligado aos derivativos, uma vez que esses nada mais são que um instrumento de transferência de risco e proteção contra a volatilidade do mercado."

Em outras palavras, está associado à conjuntura na qual a empresa está inserida, sempre sujeita a mudanças, podendo servir como exemplos a inflação e as mudanças cambiais, entre outros. Este risco é de difícil, ou mesmo impossível, eliminação, sendo apenas possível à empresa controlá-lo por meio de uma atenta análise da sua situação conjuntural (PIRES, 2010, p.20).

c) Risco operacional

No âmbito empresarial, o risco operacional compreende as deficiências na identificação dos riscos internos e o ineficiente planejamento para suportar os eventos externos. É considerado o evento mais reconhecido e predominante nas atividades humanas e empresariais.

Como descrito pelo IBGC (2007, p. 19),

> "os riscos operacionais estão associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas), resultante de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos, como catástrofes naturais, fraudes, greves e atos terroristas. Os riscos operacionais geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades, com impacto negativo na reputação da sociedade, além da potencial geração de passivos contratuais, regulatórios e ambientais."

Tais perdas são derivadas de processos internos, pessoas, sistemas ou de eventos externos. Referem-se ainda ao risco decorrente de falha de sistema, adoção de sistema inadequado para a complexidade das operações, controles ineficientes, erro humano ou falha de gerenciamento – o que poderá implicar não executar operações ou atrasá-las, causando prejuízos às partes envolvidas (FILGUEIRAS, 2007).

É fato que o risco operacional representa uma ameaça significativa ao valor de mercado das instituições financeiras (sendo esse risco utilizado no cálculo de valores futuros da empresa por parte dos potenciais investidores), principalmente no que se refere a certos tipos de riscos operacionais, como a fraude (KPMG, 2005). Ressalta-se que a atenção no risco operacional pode ser atribuída à mudança no perfil desse risco no setor de serviços financeiros, resultante de fatores como o crescimento do comércio eletrônico, a crescente dependência tecnológica deste setor, o desenvolvimento de novos produtos e serviços de elevada complexidade, e o emergente caráter global dos mercados.

2.2 Comitee of Sponsoring Organizations - COSO

Utilizando-se da contribuição de Dias (2010, p.48), cabe elucidar a respeito da importância do COSO para os estudos de gerenciamento dos riscos e controles internos, que define o significado deste comitê:

> Em 1985, foi criada nos Estados Unidos a National Commission on Fraudulent Financial Reporting (Comissão Nacional sobre Fraudes em Relatórios Financeiros), uma iniciativa independente, para estudar as causas da ocorrência de fraudes em relatórios financeiros/contábeis. Essa comissão era composta por representantes das principais associações de classe de profissionais ligados à área financeira. Seu primeiro objeto de estudo foram os controles internos. [...] Posteriormente, a Comissão transformou-se em Comitê, que passou a ser conhecido como COSO – *The Comitee of Sponsoring Organizations* (Comitê das Organizações Patrocinadoras).

O primeiro estudo do COSO ocorreu em 1992 e abordou o sistema de controles internos, dando origem à primeira publicação do comitê, definida como *Internal Control –Integrated Framework* (Controles Internos – Um Modelo Integrado), servindo de referência para os estudos de controles internos. Este *framework* é composto por elementos básicos necessários para configurar um sistema de controle interno eficaz e que permite às empresas atingirem seus objetivos. Já na ilustração do framework publicado por COSO em seu segundo trabalho, denominado de ERM, evidencia-se a adição de 3 (três) elementos: fixação de objetivos; identificação de eventos; e resposta a risco, bem como a presença dos objetivos da empresa (estratégico, operacional, comunicação e conformidade), sugerindo a reflexão de que os objetivos da empresa relacionam-se diretamente aos elementos de controle interno.

Machado e Medeiros (2013, p.345) também complementam que "o sistema de controle interno pode ser definido como conjunto de órgãos articulados a partir de um órgão central para o desempenho das atribuições de controle interno". Em síntese, os elementos apresentados fazem parte de uma rotina de controles internos com a finalidade de garantir que os objetivos da organização sejam alcançados. Estes elementos são estruturados a partir da cultura da empresa e de acordo com os riscos identificados e avaliados, para definir estratégias de tratamento e monitoramento de riscos potenciais.

3 Metodologia

a pesquisa realizada neste estudo é classificada quanto aos seguintes aspectos: (a) pela forma de abordagem do problema; (b) de acordo com seus objetivos; e (c) com base nos procedimentos técnicos utilizados.

No que tange à forma de abordagem do problema, esta pesquisa se classifica como qualitativa em função de a análise dos dados não envolver instrumentos estatísticos como base do processo de análise do problema. Beuren (2013, p. 92) destaca que "na pesquisa qualitativa concebem-se análises mais profundas em relação ao fenômeno que está sendo estudado". Assim, este estudo avaliou sob o foco qualitativo os controles internos relativos à segurança da informação de uma instituição financeira, comparando-os às normas do modelo COBIT e à literatura especializada.

De acordo com os objetivos, este trabalho se caracteriza como descritivo porque descreve os aspectos principais para a segurança informacional utilizados na instituição de estudo. Segundo Gil (2008), esse tipo de pesquisa visa à descoberta da existência de associações entre variáveis.

O estudo em pauta classifica-se, quanto aos procedimentos técnicos, como documental, tendo em vista que se utilizou de documentos e processos internos da instituição financeira estudada que ainda não sofreram tratamento analítico sob o foco desta pesquisa, utilizando o método comparativo.

Assim, por meio de um estudo de caso de uma instituição financeira, localizada no Estado do Rio Grande do Sul, foram analisadas as políticas internas relacionadas à segurança da informação, aos controles internos e aos riscos de liquidez de mercado, de crédito e operacionais, que foram comparadas aos modelos e literatura especializada.

Foi realizada uma coleta de documentos, tanto na rede colaborativa da empresa como no sítio da mesma – este último, aberto a qualquer usuário interessado –, que permitiu o efetivo desenvolvimento do estudo de caso. A coleta foi realizada nos meses de setembro e outubro de 2014.

4 Análise dos Resultados

O estudo deste trabalho foi aplicado em uma instituição financeira, localizada na região de Porto Alegre, Estado do Rio Grande do Sul. Esta empresa atua em 11 (onze) estados brasileiros e tem parcerias no mercado externo. Sua primeira sede foi inaugurada há mais de 100 anos e a instituição continua a crescer e a se expandir até os dias atuais. Como análise inicial, tomam-se alguns tópicos como parâmetros de comparação entre o modelo COBIT e a Política de Segurança Interna (PSI) da instituição financeira.

4.1 Diretrizes

A PSI da Instituição Financeira em estudo trata de algumas diretrizes para estabelecer o direcionamento estratégico e para a proteção efetiva das informações, conforme demonstrado no quadro 2, a seguir:

Quadro 2: Diretrizes da Instituição

Diretriz	Propósito
Avaliação de Riscos	Garantir a confidencialidade, integridade e disponibilidade da informação por meio de metodologia ou processo de avaliação de riscos para identificação de ameaças e vulnerabilidades.
Treinamento e Conscientização	Promover treinamentos e ações de conscientização de Segurança da Informação aos usuários para que haja ciência e concordância com as responsabilidades no cumprimento da PSI, suas normas, instruções e procedimentos.
Classificação das Informações	Classificar e proteger as informações e os ativos de informação contra acesso, divulgação, alteração ou destruição não autorizados, conforme critérios de tratamento, armazenamento, rotulação e descarte, definidos de acordo com os níveis de classificação.
Conformidade	Estar em conformidade com leis e normas vigentes e aplicáveis, especialmente aquelas que estejam relacionadas ao sigilo bancário.
Reporte de Incidentes	Comunicar à área de Segurança da Informação o descumprimento de controles estabelecidos pela PSI e todos os demais documentos que a compõem, assim como qualquer incidente ou atividade suspeita, relacionados ao uso de informações de propriedade da empresa.

Fonte: Adaptado pelos autores a partir da PSI da instituição financeira estudada.

Comparando as diretrizes do Quadro 2 com os parâmetros do modelo COBIT, pode-se afirmar que a empresa se enquadra no produto daquele modelo de "Diretrizes de Gerenciamento/ modelo de maturidade", pois auxilia na designação de responsabilidades, avaliação de desempenho e benchmark, e trata da solução de deficiências de capacidade. No item do COBIT "planejar e organizar" existe um subprocesso, chamado PO6, que trata de comunicar as diretrizes e expectativas da Diretoria que, segundo a política acima descrita, é alocado nessa etapa.

Conforme o Modelo de Maturidade mencionado no capítulo 2.2.4 - Acompanhamento da TI pela escala de maturidade do COBIT, que pertence ao subprocesso PO3 (determinar as diretrizes da tecnologia), a empresa se classificaria como "processo definido" (nível 3) pois, de acordo com o ITGI (2007, p.42), "a Direção está ciente da importância do plano de infraestrutura tecnológica. Há treinamento formal e comunicação de papéis e responsabilidades". Por meio do subprocesso PO6 temos o conceito dessa classificação como: "um ambiente completo de gestão da qualidade e controle da informação é desenvolvido, documentado e comunicado pela Direção, o qual inclui uma estrutura de políticas, padrões e procedimentos".

O ideal é a empresa sempre buscar crescer e se aperfeiçoar. Diante disso, sugere-se que a instituição procure formas de alcançar a seguir o nível de maturidade 4 (gerenciado e mensurável), utilizando ferramentas adequadas, maior controle de adesão dos procedimentos que aplica, encontrando maneiras de melhorar as falhas.

4.2. Papéis e responsabilidades

Ainda na PSI da instituição financeira estudada, as responsabilidades são distribuídas na forma do Quadro 3, conforme segue:

Quadro 3: Distribuição de Responsabilidades

Diretoria Executiva	Segurança da Informação
É responsável pela condução dos esforços estratégicos para o cumprimento dos objetivos de segurança da informação.	É responsável pela gestão e pelo direcionamento das ações de segurança da informação. Deve definir e documentar a PSI, suas normas e instruções, e garantir que os controles estabelecidos por estes documentos sejam implementados adequadamente.

Fonte: Adaptado pelos autores a partir da PSI da instituição (2014a).

Analisando o Quadro 3, verifica-se que as responsabilidades definidas pela empresa seguem a mesma linha do modelo COBIT, pois o ITGI (2007) afirma que a governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização apoie e aprimore os objetivos e as estratégias da organização.

Sobre os dois aspectos acima comparados e analisados (diretrizes e responsabilidades), a instituição está parcialmente de acordo com o modelo COBIT. Tendo em vista que a aplicabilidade do mesmo não é obrigatória, a empresa adequa à sua realidade e sua necessidade as sugestões do modelo e, conforme for expandindo no mercado, se aperfeiçoará e utilizará mais modelos de melhores práticas.

Seguindo as análises, efetua-se a comparação de literaturas referentes a controles internos e à política interna da empresa sobre esse assunto.

4.3 Controles internos

Na Política Interna da empresa são trazidos os objetivos e a utilização de um controle interno. Ao final de sua introdução, são citados os focos principais, que estão inteiramente de acordo com o COSO, quais sejam: (a) Eficácia e eficiência das operações; (b) Confiabilidade dos relatórios financeiros; (c) Cumprimento de leis e regulamentos aplicáveis.

O Comitê da Basileia (2006) apresenta os princípios para um bom gerenciamento de controles internos. O primeiro deles trata das responsabilidades da alta administração. Na Política Interna analisada consta que a Diretoria Executiva é responsável pela aprovação da Política de Controles Internos e *Compliance*; logo, está de acordo com a lei nesse aspecto. Também o Conselho de Administração é o órgão que, em nível estratégico, aprova esta, bem como suas revisões e alterações.

O Quadro 4 demonstra as responsabilidades da Superintendência de Controles Internos com relação aos controles internos comparados aos princípios do Comitê da Basileia, conforme segue:

Quadro 4: Responsabilidade da Superintendência de Controles Internos x Princípios do Comitê da Basileia.

	Responsabilidades da Superintendência*	Princípio da Basileia**
1	Disseminar a cultura de controles internos no Sistema, englobando o conjunto de políticas internas, normas externas, comportamentos, conhecimentos e recursos aplicados pelos colaboradores de todos os níveis nos negócios, serviços e atividades do Sistema.	Princípio 3
2	Disponibilizar ferramentas e diretrizes ao Sistema para efetuar a avaliação de controles internos, com base em metodologias internacionalmente aceitas (exemplo: COSO).	Princípio 1
3	Conduzir o alinhamento das atividades de controles internos com as demais disciplinas de gerenciamento de riscos, especialmente com a de risco operacional.	Princípios 4 e 17
4	Validar o planejamento anual de auditoria interna.	Princípios 12 e 17

Fonte: Adaptado pelos autores, a partir da Política Interna de Controles Internos e Compliance da Instituição estudada e de ASSI (2010, p.50 - 62).

Analisando o primeiro aspecto do Quadro 4, está de acordo com o Princípio 3 de Basileia, que afirma que uma das responsabilidades da alta administração é estabelecer uma cultura organizacional que enfatize e demonstre a todos os níveis do pessoal a importância dos controles internos.

O segundo aspecto se adequa ao Princípio 1, tendo em vista que o mesmo enfatiza que a administração deve fornecer diretrizes e orientações à gerência de nível superior e supervisioná-las. O terceiro item assemelha-se ao Princípio 4, postulando que um sistema de controles internos efetivo requer que os riscos materiais que poderiam afetar adversamente a realização dos objetivos da empresa sejam reconhecidos e continuamente avaliados.

Por último, o quarto tópico elucida o Princípio 12, que prevê uma auditoria interna executada por pessoal adequadamente treinado, competente e operacionalmente independente. Essa equipe deve monitorar os controles internos da empresa e reportar-se à Superintendência, neste caso.

Após as análises acima descritas, conclui-se que a empresa tem um bom sistema de controles internos e tenta se aproximar ao que o COSO e o Comitê da Basileia aconselham às empresas para que mantenham a sua continuidade e crescimento no mercado.

4.4 Comparativo entre os preceitos da literatura contábil quanto aos riscos

Nesta seção, analisaremos os três tipos de riscos citados anteriormente, segundo definições do COSO, normas e resoluções, e os compararemos com as políticas de gerenciamento dos riscos da empresa.

a) Gerenciamento de Riscos

Segundo definição do COSO, toda organização enfrenta incertezas e o desafio de sua administração é determinar o nível de incerteza que a empresa está preparada para aceitar, na medida em que se empenha em agregar valor para as partes interessadas. O gerenciamento de riscos corporativos não apenas permite identificar, avaliar e administrar riscos diante de incertezas, como também integra o processo de criação e preservação de valor.

De acordo com a Política de Gerenciamento de Riscos da instituição financeira, o gerenciamento de riscos corporativos é um processo conduzido pelo Conselho de Administração, pela Diretoria Executiva e pelos demais empregados ligados ao estabelecimento de estratégias por meio de toda a organização. Além de ser capaz de identificar eventos em potencial (como é indicado no COSO), capazes de afetar a organização, o processo permite o gerenciamento de riscos de forma compatível com o apetite a risco da organização e, ainda, possibilita um nível razoável de garantia em relação à realização dos seus objetivos.

b) Risco de Mercado e de Liquidez

Na Política Interna consta que o gerenciamento do risco de mercado consiste no processo de identificação e avaliação dos riscos existentes ou potenciais e no seu efetivo monitoramento e controle, conduzidos por meio da adoção de políticas e processos de gestão, de limites consistentes com as estratégias de negócios e de metodologias voltadas à sua administração e à alocação de capital econômico compatível com as exposições incorridas.

A Política de Risco de Mercado da instituição estudada descreve a estrutura e o conjunto de métodos, processos e diretrizes adotados com vistas a garantir o adequado gerenciamento das exposições, assim como a sua manutenção em níveis compatíveis com as estratégias e o apetite a risco de mercado do sistema, atendendo à Resolução CMN 3.464, de 26 de junho de 2007, que estabelece as principais exigências relativas ao Risco de Mercado.

A empresa estudada realiza a análise dos riscos conforme segue:

- Análises Diárias: cálculos de risco de mercado para as carteiras, especialmente as de negociação (*trading*);
- Análises Mensais: cálculos de risco de mercado relativos às carteiras de não negociação (*banking*);
- Demais Análises: análises adicionais realizadas sempre que necessário, seja em função de novas exposições, seja em função de alterações nos cenários de mercado que possam impactar as exposições incorridas.

Em atendimento à Resolução nº 4.090 do CMN e à Circular nº 3.393 do BACEN, a instituição possui estrutura de gerenciamento do risco de liquidez compatível com a natureza das operações, a complexidade dos produtos e a dimensão da exposição ao risco de liquidez do sistema.

O gerenciamento do risco de liquidez está centralizado sob uma unidade específica responsável pelo monitoramento do risco de liquidez do Sistema. O atendimento aos normativos e controle de liquidez é realizado por meio dos seguintes instrumentos e ferramentas que são reportados às demais áreas e entidades interessadas:

- Projeções de Liquidez (fluxo de caixa);
- Teste de Estresse;
- Limites de Liquidez;
- Plano de Contingência de Liquidez.

c) Risco Operacional

A estrutura centralizada de gerenciamento de risco operacional está implementada na Superintendência de Controles Internos, *Compliance* e Risco Operacional da instituição, subordinada diretamente à Presidência Executiva.

Essa estrutura é responsável pela administração da política e pela coordenação e execução, no que lhe compete, dos processos relativos à disciplina para todo o sistema, de forma padronizada e centralizada. A Auditoria Interna é área independente desta estrutura, sendo responsável pela verificação das atividades relacionadas ao risco operacional.

As políticas de gerenciamento do risco operacional são analisadas e validadas pela Diretoria Executiva e pelo Conselho de Administração, sendo sua revisão realizada pelo menos uma vez ao ano. O documento estabelece, entre outros, a forma de organização, as diretrizes e os papéis e responsabilidades relacionados a esta disciplina. Além da Política, a Metodologia de Gerenciamento do Risco Operacional padroniza os conceitos e métodos vinculados a este tema para toda a organização.

O processo de gerenciamento do risco operacional é desenhado para capacitar a identificação, avaliação, mitigação e monitoramento dos riscos associados à instituição. Trata-se de um ciclo integrado compreendido por um conjunto de etapas que visa a manter a exposição ao risco operacional em níveis toleráveis, avaliados constantemente pela alta administração. O ciclo de gerenciamento do risco operacional contempla as seguintes fases: a) identificação de risco operacional; b) identificação de controles; c) avaliação de controles; d) mitigação do risco operacional; e) monitoramento do risco operacional.

Todo o ciclo de gerenciamento do risco operacional é apoiado por ferramenta sistêmica que integra as informações e possibilita o monitoramento centralizado do risco em todas as entidades do Sistema, financeiras e não financeiras.

5. Conclusões

O presente estudo comparou as práticas da segurança da informação e dos controles internos preceituadas pela literatura especializada, com a realidade de uma instituição financeira, localizada no Estado do Rio Grande do Sul, com vista à prevenção de riscos. Para tanto, valeu-se da análise das políticas internas da instituição comparadas com os modelos preceituados pela literatura contábil especializada, efetuando-se um estudo comparativo dos documentos coletados sob o foco qualitativo, por meio de método descritivo.

Assim sendo, este estudo teve como objetivo responder à seguinte questão de pesquisa: qual é o nível de conformidade da segurança da informação e dos controles internos para a prevenção de riscos em uma instituição financeira? Frente a essa questão, constata-se que, com relação à segurança da informação, a instituição estudada tem uma organização adequada e em fase de consolidação, proporcional às suas finalidades comerciais. Entretanto, a mesma não se encontra inteiramente de acordo com o modelo COBIT, visto que este não é um instrumento obrigatório, apenas reúne práticas aconselháveis às instituições financeiras pelo Banco Central do Brasil (BACEN).

Após esta análise, identificou-se que a instituição estudada encontra-se no nível de maturidade 3, ou seja, a Direção está ciente da importância do plano de infraestrutura tecnológica, há treinamento formal e comunicação de papéis e responsabilidades, mas ainda não está suficientemente estruturada para enquadrar-se no nível 4 de maturidade. É importante que a organização encontre maneiras de adequar-se aos níveis superiores e esteja em constante evolução para que, no futuro, possa alcançar o nível mais elevado de maturidade (nível 5) nos controles internos e governança de TI.

Comparada aos princípios do Comitê da Basileia, a instituição em estudo tem as responsabilidades da Superintendência de acordo com alguns desses itens e se preocupa em manter um bom nível de eficácia e eficiência das operações, confiabilidade dos relatórios financeiros e cumprimento de leis e regulamentos aplicáveis. Esses últimos, adequados aos objetivos indicados pelo COSO.

O gerenciamento dos riscos é efetuado segundo as definições do COSO, sendo os riscos inerentes ao ramo financeiro analisados conforme preceitos deste comitê. A empresa determina diretrizes para os três tipos de riscos analisados (mercado, liquidez e operacional), cada um com sua complexidade e peculiaridade.

Embora o presente trabalho tenha limitações, tem-se em mente que este estudo constitui-se em uma contribuição para ampliar o conjunto de publicações de estudos e dados sobre formas de se manter o controle de suas informações financeiras, evitar riscos inerentes ao ramo e manter a segurança nos negócios, dando continuidade às organizações. Com essas informações, espera-se que não só as instituições financeiras, como as empresas em geral, possam refletir e implementar métodos de controles internos atualizados e coerentes. Dessa forma, com os sistemas avançados e eficientes de segurança da informação, o controle dos riscos dos negócios poderá ser reduzido.

Sugere-se para trabalhos futuros uma pesquisa quantitativa sobre os riscos de uma instituição financeira, com vistas a aprofundar a análise de diretrizes e formas de redução dos mesmos, mantendo os controles e a segurança das informações atualizados e em conformidade com o ramo da empresa e a evolução do mercado.

Referências

ADLER, R. W.; MILNE, M. J. **Improving the quality of accounting students' learning through action-oriented learning tasks**. Accounting EdANTUNES, Jerônimo. Modelo de Avaliação de Risco de Controle Utilizando a Lógica Nebulosa. 2004, 162 f. (Tese de Doutorado em Contabilidade e Controladoria) – Faculdade de Economia, Administração e Contabilidade – Universidade de São Paulo, 2004.

ASSI, Marcos. **Controles internos e cultura organizacional: como consolidar a confiança na gestão dos negócios**. 1ª ed. São Paulo: Saint Paul, 2012.

BACEN - BANCO CENTRAL DO BRASIL. **Resolução Nº. 2.682, de 22 de dezembro de 1999**. Dispõe sobre os critérios de classificação das operações de crédito e regras para constituição de provisão para créditos de liquidação duvidosa. Disponível em: < www.bcb.gov.br/ >. Acesso em 24 nov. 2014.

BACEN - BANCO CENTRAL DO BRASIL. **Circular Nº 3.393, de 03 de julho de 2007**. Dispõe sobre o controle do risco de liquidez e estabelece procedimentos para remessa de informações. Disponível em: < www.bcb.gov.br/ >. Acesso em 24 nov. 2014.

BACEN - BANCO CENTRAL DO BRASIL. **Resolução N° 3.464, de 26 de junho de 2007**. Dispõe sobre a implementação de estrutura de gerenciamento do risco de mercado. Disponível em: < www.bcb.gov.br/ >. Acesso em 26 nov. 2014.

BACEN - BANCO CENTRAL DO BRASIL. **Resolução Nº 4.090, de 24 de maio de 2012**. Dispõe sobre a estrutura de gerenciamento do risco de liquidez. Disponível em: < www.bcb.gov.br/ >. Acesso em 23 nov. 2014.

BEUREN, Ilse Maria. **Como elaborar trabalhos monográficos em Contabilidade: teoria e prática**. 3ª ed. São Paulo: Atlas, 2013.

CAOUETT, John. B. et al. **Gestão do risco de crédito: O grande desafio dos mercados financeiros globais**. 2ª ed. Rio de Janeiro: Qualitymark, 2009.

CFC - CONSELHO FEDERAL DE CONTABILIDADE. **Resolução CFC n.º 750, de 29 de dezembro de 1993**. Dispõe sobre os Princípios de Contabilidade (PC). Diário Oficial [da República Federativa do Brasil], 31 dez. 1993 Disponível em: <http://www.portaldecontabilidade.com.br/legislacao/resolucaocfc774.htm>. Acesso em: 15 jun. 2015.

COMITÊ DA BASILÉIA PARA SUPERVISÃO BANCÁRIA. P**rincípios Fundamentais para uma Supervisão Bancária Efetiva (Os Princípios Fundamentais da Basiléia)**. Outubro de 2006. Disponível em: < http://www.bcb.gov.br/fis/supervisao/docs/Core_Principles_Traducao2006.pdf>. Acesso em: 15 novembro 2015.

DAMODARAN, Aswath. **Gestão estratégica do risco: uma referência para a tomada de riscos empresariais**. Porto Alegre: Bookman, 2009.

DIAS, Sergio Vidal dos Santos. **Auditoria de Processos Organizacionaias: teoria, finalidade, metodologia de trabalhos e resultados esperados**. 2 ª ed. São Paulo: Atlas, 2010.

FILGUEIRAS, Claudio. **Manual da Contabilidade Bancária: mais de 300 questões com gabarito**. 3ª ed. Rio de Janeiro: Elsevier.2010.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 6ª ed. São Paulo: Atlas, 2008.

GRAZZIOTIN, Carlos Augusto. **Controles Internos e Gestão de Riscos em instituições financeiras. 2002**. 75 f. Dissertação (Mestrado em Economia com ênfase em Controladoria) – Curso de Pós-Graduação em Economia da Faculdade de Ciências Econômicas da UFRGS, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2002.

IBGC. **Guia para melhorar a governança corporativa através de eficazes controles internos**. 2007 Disponível em <http://www.ibgc.org.br/BibliotecaDetalhes.aspx?CodAcervo=193 .> Acesso em 25 jan. 2015.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das melhores práticas de governança corporativa**. 4ª ed. São Paulo, 2010.

ITGI - IT GOVERNANCE INSTITUTE. **COBIT 4.1**: Rolling Meadows, Illinois, EUA, 2007.

KPMG. **Managing Operational Risk Beyond Basell II**. KPMG Financial Services. 2005.

LUCIANO, Edimara Mezzomo et al. **Aplicabilidade do COBIT na gestão de atividades de tecnologia da informação terceirizadas: uma investigação com base em duas empresas multinacionais**. Revista Eletrônica de Sistemas de Informação, v. 9, nº 2, artigo 6, 2010.

MACHADO, Caren Silva; MEDEIROS, André Amaral. **A Importância do Sistema de Controle Interno para Garantia da Transparência e da Qualidade das Informações**. Unoesc International Legal Seminar, Chapecó, v. 2, nº 1, p. 339-355, 2013.

NASCIMENTO, V. P.; ALVES, C. A. M. **Avaliação de modelo de gerenciamento de riscos corporativos segundo recomendações do IBGE: caso Brasil TELECOM**. Revista Eletrônica de Ciência Administrativa, v. 6, nº 2, p. 1-13, 2007.

NEVES, Wesley Christian Gonçalves das. **Diretrizes para Implantação da Governança de Tecnologia da Informação com Base no COBIT, a Partir da ISSO 9001: aspectos de gerenciamento de projetos**. 2007. 128 f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) – Curso de Pós-Graduação em Gestão do Conhecimento e da Tecnologia da Informação, Universidade Católica de Brasília, Brasília, 2007.

PIRES, José Pedro. **Contributo da Auditoria Interna na Detecção e Mitigação de Riscos Empresariais**. 2010. 81 f. Dissertação (Mestrado em Auditoria) – Pós-Gradução em Gestão, Instituto Superior de Contabilidade a Administração de Lisboa, Lisboa, 2010.

TRAPP, Adriana Cristina Garcia; CORRAR, Luiz J. **Avaliação e gerenciamento do risco operacional no Brasil: análise de caso de uma instituição financeira de grande porte**. Revista Contabilidade e Finanças, v.16, nº 37. São Paulo, jan/abr 2005.

TUTTLE, Brad; VANDERVELDE, Scott D. **An Empirical Examination of COBITT as an Internal Control Framework for Information Technology**. International Journal of Accounting Information Systems, nº 8. Columbia; Sept. 2007.