# FACULDADES IBMEC

**PROGRAMA DE PÓS-GRADUAÇÃO E PESQUISA EM**

**ADMINISTRAÇÃO E ECONOMIA**


# UMA CONTRIBUIÇÃO PARA A AVALIAÇÃO DO SISTEMA DE CONTROLES INTERNOS EM UMA INSTITUIÇÃO FINANCEIRA COM FOCO EM OPERAÇÕES DE TESOURARIA

**Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Administração e Economia das Faculdades Ibmec como requisito à obtenção do título de Mestre em Economia**


**SANDRO LOPES DA COSTA CUPELLO**

**ORIENTADOR: ANTONIO MARCOS DUARTE JUNIOR**

**CO-ORIENTADOR: JOSE SANTIAGO FAJARDO BARBACHAN**



RIO DE JANEIRO (RJ)

AGOSTO/2006

**“UMA CONTRIBUIÇÃO PARA A AVALIAÇÃO DO SISTEMA DE CONTROLES INTERNOS EM UMA INSTITUIÇÃO FINANCEIRA COM FOCO EM OPERAÇÕES DE TESOURARIA”**

**SANDRO LOPES DA COSTA CUPELLO**

Dissertação de Mestrado Profissionalizante apresentada ao Programa de Pós-Graduação em Administração e Economia das Faculdades Ibmec, como requisito parcial necessário para a obtenção do título de Mestre em Economia.
Área de Concentração: Finanças.

Aprovada em 01 de agosto de 2006.

**BANCA EXAMINADORA**

## FICHA CATALOGRÁFICA

__ Cupello, Sandro Lopes da Costa.
Uma contribuição para a avaliação do sistema de controles internos em uma instituição financeira com foco em operações de Tesouraria / Sandro Lopes da Costa Cupello. Rio de Janeiro: Faculdades Ibmec, 2006.

Dissertação de Mestrado Profissionalizante apresentada ao Programa de Pós-Graduação em Economia como requisito parcial necessário para a obtenção do título de Mestre em Economia.

Área de concentração: Finanças

1. Instituição Financeira. 2. Operações de Tesouraria. 3. Avaliação de Controles Internos. 4. Economia – Teses.

A minha esposa Tatiana que nesses últimos 10 anos foi a minha grande força e a nossa filha Pietra que é a nossa maior recompensa.

## AGRADECIMENTOS

Aos meus amigos Luiz Fernando Parente, Antonio Paulo Sodré e Elizabeth Lott que sempre confiaram em mim e me deram a oportunidade de conquistar essa vitória pessoal e profissional.

Ao professores Antonio Marcos Duarte e Jose Fajardo, meu muito obrigado pela orientação e incentivo.

Ao meu colega de mestrado, colega de MBA, colega de faculdade, proa de barco, companheiro de corrida, cumpadre e irmão Rogério por todo apoio que você me dá.

A minha mãe Rosangela e pai Paulo pelo amor, paciência, esforço e união com que criaram a mim e meus irmãos.

A minha família e amigos, em especial, ao João Paulo, Cristiane, Cristina, Paula, Thiago, Janine, Monica, Renato e Luis.

Aos meus amores Tatiana e Pietra Cupello que mesmo sentindo muito minha falta, sempre me incentivaram. Sem vocês, com certeza, nada disso seria possível.

Enfim, obrigado a todos que, direta ou indiretamente, contribuíram para a realização desse trabalho.

## RESUMO

O risco de uma instituição financeira não gerir seus problemas potenciais de forma devida é a preocupação fundamental dos acionistas, Alta Administração, órgãos reguladores, credores e demais participantes do mercado.

Para assegurar-se que esses problemas potenciais são controlados de forma confiável e adequados por um sistema de controles internos, a Alta Administração delega a profissionais especializados, tais como, auditores, compliance officers, gestores de qualidade, entre outros, a responsabilidade por avaliar a segurança desses controles.

A contribuição deste trabalho está na apresentação de questões relevantes na avaliação da qualidade dos controles internos em uma instituição financeira com foco em operações de Tesouraria. Desta forma, a dissertação é voltada principalmente aos membros de Comitês de Governança Corporativa, auditores internos e externos, compliance officers e gestores da qualidade, que são responsáveis por monitorar os sistemas de controles internos.

São diversas questões relevantes que esse trabalho busca elucidar, tais como: Quais são as normas brasileiras e internacionais que orientam ou regulam essa matéria? Quais são as metodologias disponíveis para realização dessas avaliações? Que riscos são relevante em qualquer instituição financeira? Que testes devem ser realizados para avaliação desses controles?

Esse trabalho avalia as possíveis respostas a tais questões, mencionando elementos que podem contribuir para um melhor entendimento do processo de gestão de riscos.

## ABSTRACT

The risk of not managing its risks properly is a critical issue to the shareholders, Senior Management, regulators, creditors and other participants.

In order to ensure if the potential problems are controlled effectively and properly by an internal system control, the Senior Management mandate to a special staff, such as, internal auditors, compliance officers and others, the responsibilities to assess these controls.

The contribution of this work is to present relevant issues regarding the evaluation of the quality of the internal controls in a financial institution focused on Treasury activities. Therefore, this work is addressed, especially, to members of Corporate Governance Committee, internal and external auditors and compliance officers who are in charge of assessing the internal system control.

There are several questions that this work searches to clarify, such as: What are the Brazilian and international legislation that oriented or rule this matter? What are the methodologies disposed to perform this evaluation? What are the relevant risks incurred by any financial institution? What tests must be performed to assess the controls?

The present study explores the possible answers to such questions, mentioning elements, which may contribute for a better understanding of the risk management.

1- Introdução ..... 13
1.1 – Exposição do tema ..... 13
1.2 – Objetivo ..... 17
1.3 – Motivações ..... 18
1.4 - A Importância do Problema ..... 21
1.5 – Estrutura da Dissertação ..... 24
2- Controles Internos em instituições financeiras ..... 26
2.1- Introdução ..... 26
2.2- Controles internos ..... 30
2.2.1- COSO: *Internal Control: Integrated Framework* ..... 32
2.2.2- SAS 55/78 – *Statement on Auditing Standard* ..... 35
2.2.3 - *Systems Auditability Control Report (SAC)* ..... 37
2.2.4- *Control Objetives for Information and related Technology* (CobiT) ..... 38
2.2.5- Considerações ..... 40
3- Metodologia ..... 43
3.1- Definição do Escopo ..... 44
3.2- Entendimento do negócio ..... 46
3.3- Identificação dos riscos ..... 54
3.4- Elaboração de programa de trabalho ..... 58
3.4- Execução dos testes dos controles ..... 60
3.5- Emissão dos relatórios ..... 61
4 - Avaliaçao do Ambiente de Informática ..... 64
4.1- Planejamento e Organização ..... 66
4.1.1- Plano estratégico de TI ..... 66
4.1.2- Definição de arquitetura das informações ..... 67
4.1.3- Determinação da direção tecnológica ..... 68
4.1.4- Definição da organização e as relações de TI ..... 68
4.1.5- Administração dos investimentos de TI ..... 69
4.1.6 – Comunicação dos objetivos e direção da administração ..... 70
4.1.7- Cumprimento dos requisitos externos ..... 71
4.1.8 – Gerenciamento dos projetos ..... 72
4.2 – Aquisição e implementação ..... 74
4.2.1 - Identificação das Soluções Automatizadas ..... 74
4.2.2 – Instalar e aprovar sistemas ..... 76
4.2.3 – Gerenciar mudanças ..... 77
4.3 – Entrega e Suporte ..... 79
4.3.1 – Definir e gerenciar os níveis de serviço ..... 79
4.3.2 – Gerenciar os serviços de terceiros ..... 80
4.3.3 – Gerenciar o desempenho e a capacidade ..... 81
4.3.4 – Garantir a continuidade do serviço ..... 81
4.3.5 - Garantir a segurança dos sistemas ..... 82
4.3.6 – Gerenciamento dos dados ..... 85
4.3.7 – Gerenciamento das instalações ..... 86
4.4 – Monitoramento ..... 87
4.4.1 – Monitorar os processos ..... 87
5 – Avaliação da Gestão do Risco de Mercado ..... 88
5.1 – Limites de Riscos de Mercado ..... 88
5.1.5 - Eficiência ..... 93

5.1.6 – Formalizaçao ..... 94
6- Avaliação da Gestao do Risco de Liquidez ..... 95
6.1 – Fluxo de Caixa ..... 97
6.2- Plano de contingência de liquidez ..... 98
6.3- Modelagem do Risco de Liquidez ..... 99
7 – Avaliaçao do Risco de Modelagem ..... 102
7.1- Value-at-Risk ..... 104
7.1.1- Escolha das premissas ..... 104
7.1.2- Mapeamento dos fatores de risco ..... 108
7.1.3- Cálculo da volatilidade ..... 113
7.1.4- Cálculo da correlação ..... 114
7.2- Teste de estresse ..... 115
7.2.1- Subjetividade ..... 116
7.2.2- Opcionalidade ..... 117
7.2.3- Deslocamentos nao paralelos da curva de juros ..... 117
7.3- Back-test ..... 118
7.3.1- Taxa e independência das falhas ..... 118
7.3.2- Base de avaliação do resultado ..... 119
7.4- Apreçamento ..... 121
8- Avaliação do Risco de Informação para Tomada de Decisão ..... 124
9- Avaliação da Gestão do Risco de Crédito ..... 126
10- Risco Legal ..... 128
10.1 – Risco de legislação ..... 128
10.2- Risco Tributário ..... 131
10.3- Risco de Contrato ..... 136
11- Outros Riscos ..... 136
11.1- Padrões éticos ..... 137
11.2 – Política de Remuneração Variável ..... 137
11.3- Segregação de funções ..... 138
11.4 – Registro e formalização das operações ..... 139
11.5- Confirmação das operações ..... 140
11.6- Liquidação das operações ..... 141
11.7- Procedimentos de conciliação ..... 141
11.8- Conflito de interesse ..... 142
12. Conclusão ..... 144

## LISTA DE TABELAS


Tabela 1 - Atuação da auditoria interna na revisão dos riscos de tesouraria

Tabela 2 - Histórico de Perdas Operacionais

Tabela 3 - Foco de atuação da Auditoria Interna na revisão dos riscos de tesouraria

Tabela 4 - Resumo da estrutura da área de Tesouraria

Tabela 5 - Principais subáreas do risco de mercado

Tabela 6 - Principais subáreas do risco operacional

Tabela 7 - Principais subáreas do risco de crédito

Tabela 8 - Principais subáreas do risco legal

Tabela 9 - Cálculo do VaR pelos diferentes metodologias

Tabela 10 - Mapeamento dos fatores de risco

Tabela 11 - Ordem de relevância na exposição dos riscos


## LISTA DE ANEXOS


Anexo 1 - Princípios Essenciais para uma supervisão bancária eficaz

Anexo 2 - 13 Princípios para a avaliação de sistemas de controles internos

Anexo 3 - Histórico das atividades de Compliance


## LISTA DE APÊNDICES


Apêndice 1 - Guia rápido de perguntas


## LISTA DE FIGURAS


Figura 1 - Estrutura tridimensional integrada do COSO

Figura 2 - Estrutura da Tesouraria

Figura 3 - Utilização da matriz de riscos pela Auditoria Interna

Figura 4 - Freqüência de avaliação pela Auditoria Interna dos controles

Figura 5 - Procedimentos de revisão na área de tesouraria e gestão de riscos

## 1- Introdução

### 1.1 – Exposição do tema

O Sistema de Controles Internos compreende as políticas e procedimentos instituídos pela Alta Administração de uma instituição financeira, para assegurar que os riscos inerentes às suas atividades sejam identificados e geridos adequadamente.

Em 1974 foi criado o Comitê de Supervisão da Basiléia - Comitê para supervisionar as instituições financeiras e, em 1997, o Comitê emitiu os 25 Princípios para Fiscalização Bancária Eficaz (Anexo 1) para fortalecer a solidez dos sistemas financeiros. Em 1998, o Comitê publicou os 13 princípios para avaliação dos sistemas de controles internos (Anexo 2).

Com base nas recomendações do Comitê, o Banco Central do Brasil editou norma (Resolução 2554/98) que dispõe sobre a necessidade de implantação e implementação de Sistema de Controles Internos.

Define, ainda, no parágrafo 2º daquela norma, como responsabilidade da Alta Administração: a) a implantação e a implementação de uma estrutura de controles internos efetiva mediante a definição de atividades de controle para todos os níveis de negócios da instituição; b) o estabelecimento dos objetivos e procedimentos pertinentes aos mesmos; c) a verificação sistemática da adoção e do cumprimento dos procedimentos definidos em função do disposto no inciso II.

Segundo o Manual da Supervisão do BACEN, um elemento fundamental da abordagem prudencial observada pela Supervisão é que as instituições financeiras devem ter controles internos adequados e efetivos. De fato, a verificação da cobertura e eficácia destes controles, à luz das diretrizes em vigor e das boas práticas geralmente aceitas, é uma parte significativa de qualquer inspeção dos órgãos reguladores em uma instituição financeira.

Cabe salientar que os Controles Internos permeiam todas as operações e atividades de uma instituição financeira.

A verificação de exposição a riscos e do atendimento aos regulamentos não será completa, portanto, sem uma adequada avaliação da cobertura e efetividade dos controles internos. Faz-se necessário mapear os grandes riscos e avaliar a gestão dos riscos de mercado, crédito e operacional pelas instituições financeiras.

A implantação de um sistema de controles internos, nos moldes estabelecidos pela Resolução 2.554 do Bacen tornou-se, tanto uma obrigação regulamentar a ser seguida, como também fundamental para as instituições financeiras nos últimos anos.

Pesquisar e compreender a nova realidade econômica financeira mundial, os avanços tecnológicos, a criação de novos produtos e serviços e os demais fatores que afetam as instituições financeiras, tornou-se vital no processo de gerenciamento de risco. Desta forma, os controles e o respectivo processo de avaliação dos mesmos, devem acompanhar essas mudanças na forma com que administram ou devem administrar os riscos.

Diante desta realidade, evidenciada com a quebra de grandes instituições, como Barings Bank, Banco BCCI, Banco Nacionale del Lavoro, aquelas instituições financeiras que não possuírem departamentos de controles internos bem estruturados, tais como, Auditoria Interna, Compliance, Controles Internos, Qualidade, entre outros, terão que ajustar-se ou estarão incorrendo em riscos que podem ser de magnitude catastrófica.

Cruz (2003) ressalta que, no passado, os bancos focavam seus esforços nas áreas de negócio, especialmente no desenvolvimento de operações financeiras complexas, sendo relativamente comum, a negligência pelas áreas de processamento e controle das operações. Desse modo, esse problema cultural aumenta o risco de perdas operacionais.

A Tabela 1 abaixo demonstra exemplos de perdas incorridas por instituições financeiras.

Tabela 1 – Histórico de Perdas Operacionais

| **Instituição** | Atividade | Período | **Perda em US$ milhões** |
|---|---|---|---|
| Daiwa Bank | Negociação não-autorizada de bônus devido a maus controles gerenciais | 1984-95 | 1.100 |
| Crédit Lyonnais | Mau controle de empréstimos | Anos 80 e 90 | 29.000 |
| Kidder Peabody | Negociação de bônus falta de controles internos. | 1994 | 200 |
| Morgan Grenfell | Falsidade ideológica | Década de 90 | 640 |
| Condado de Orange | Negociação de bônus falta de supervisão gerencial. | 1994 | 1.700 |
| Barings, Cingapura | Controle inadequado de negociação de futuros – especialmente má segregação de tarefas | 1995 | 1.600 |
| Deutsche Bank, Londres | Investimento fora de alçada | 1996 | 600 |

Fonte: Marshall (2002)

## 1.2 – Objetivo

O objetivo desta dissertação está relacionado às explorações de práticas e dos principais *issues* inerentes às instituições financeiras com foco em operações de Tesouraria e na avaliação dos sistemas de controles internos, dos auditores, compliance officers, gestores de risco e órgãos reguladores.

Neste contexto, é necessária a abordagem dos seguintes temas:

Inserção dos gestores responsáveis pelos controles internos nas instituições financeiras,

- Apresentação de uma metodologia de atuação, com a descrição das etapas dos processos e dos principais temas que os gestores dos controles internos devem focar;
- Sugerir a abordagem de fatores críticos na avaliação dos controles internos de uma instituição financeira com foco em operações de Tesouraria.

A dissertação não tem a pretensão de ser dirigida aos gestores de riscos de mercado, crédito ou operacional, mas sim àqueles que, mesmo não sendo parte integrante das rotinas operacionais da gestão direta destes riscos, têm a difícil tarefa de avaliar os controles internos e a atuações dos gestores.

Neste contexto, a dissertação é voltada, principalmente, aos membros de Comitês de Governança Corporativa, auditores internos e externos, compliance officers e gestores da qualidade, que são responsáveis por monitorar os sistemas de controles internos

## 1.3 – Motivações

O desenvolvimento de controles internos, a aferição de sua eficiência e eficácia, é condição *sinequanon* para a atuação das instituições financeiras, dado, entre outros fatores, a obrigatoriedade regulamentar, o significativo volume de recursos envolvidos, a volatilidade do mercado, a competição entre os bancos e a alocação de capital.

Neste contexto, Duarte e Lelis (2002) mencionam que o surgimento de áreas para o gerenciamento de riscos com uma visão corporativa é um passo necessário para a efetiva alocação de capital. Ainda segundo os autores, as áreas de gerenciamento de riscos com visão corporativa são as mais habilitadas para a identificação, o mapeamento, a medição e a consolidação das exposições a riscos.

No passado este trabalho foi feito no Brasil em parte pelas Auditorias Internas, mas, por questões de segregação de atividade, já não o é mais.

Caberia, então, a Auditoria Interna, a responsabilidade de avaliar a qualidade e efetividade do gerenciamento dos riscos corporativos, através da avaliação dos seus respectivos controles. Esse processo de avaliação é o que chamamos de verificação da qualidade dos sistemas de controles internos. Ressaltamos que a responsabilidade pela avaliação da qualidade e efetividade dos controles internos pode estar em diversas áreas, dependendo da instituição financeira, com destaque, além da Auditoria Interna, as áreas de Controles Internos, Compliance, Qualidade, entre outros.

Por fatores que exploraremos ao longo da dissertação, estes departamentos não estão envolvidos diretamente com a gestão efetiva dos riscos e geralmente os profissionais que atuam nestas áreas são generalistas e, portanto, seu conhecimento dos riscos é inferior aos gestores dos processos, uma vez que os mesmos não são diretamente envolvidos com as operações.

A responsabilidade de avaliar a eficiência e eficácia dos controles internos é um processo que, entre outros, inclui a discussão com os gestores das demais áreas que, certamente, possuem um conhecimento técnico muito mais profundo dos riscos envolvidos, até a sugestão de recomendações.

Desta forma, podemos afirmar que a realização de um trabalho de qualidade, com a sugestão de recomendações relevantes para todas as áreas da instituição, discussão em elevado nível técnico com os gestores e a emissão de relatórios que atendam de forma satisfatória aos diversos leitores são tarefas extremamente árduas.

Certamente já foi muito mencionado a importância de um sistema de controles internos no contexto de controle e gerenciamento de riscos. Contudo, pouco foi efetivamente apresentado, sob um contexto prático, de como devem ser realizados a avaliação e implementação dos controles internos de uma instituição financeira com foco em operações de tesouraria com a apresentação de testes detalhados.

Seguindo a tendência de emitir normativos que abordem conceitos, o próprio Bacen na Resolução 2.554 é muito pouco prático e, independente dos motivos, é

limitada sua contribuição para a descrição de como deve ser efetivamente avaliado o tão discutido conceito de sistema de controles internos.

## 1.4 - A Importância do Problema

A internacionalização dos conhecimentos, com o crescimento da sofisticação da tecnologia bancária e desenvolvimento de modelos matemáticos cada vez mais elaborados, tornaram as atividades e os riscos cada vez mais complexos e difíceis de serem avaliados.

Uma análise das falhas que geraram as perdas sofridas pelas instituições financeiras indica que estas poderiam provavelmente ter sido evitadas se as mesmas mantivessem sistemas de controles internos eficazes. Tais sistemas poderiam ter impedido ou detectado com antecedência os problemas que resultaram em perdas.

Segundo Correia (2005) falências como a ocorrida com o Barings em 1995, aumentou a preocupação de órgãos internacionais com o fortalecimento dos controles internos e, neste contexto, o estudo de casos como este evidenciam que as perdas ocorreram em função de sistemas de controles internos ineficientes.

Arcoverde (1999) menciona que as autoridades regulamentares brasileiras têm mostrado preocupação crescente com a gestão das tesourarias. Nos últimos anos, houve uma evolução contínua do ambiente regulamentar no Brasil, relativo às operações de tesouraria, incluindo requerimento de capital crescente para enfrentar a alta volatilidade dos mercados locais.

Neste contexto, o Comitê de Basiléia, juntamente com supervisores da área bancária em todo o mundo, enfatiza cada vez mais a importância de controles internos

sadios. Este forte interesse é, em parte, resultado das perdas significativas incorridas por diversas organizações bancárias nos últimos tempos.

De outra parte, em PricewaterhouseCoopers (2005), baseada em 258 entrevistas com CEOs, há consenso bastante amplo (86%) entre os CEOs sul-americanos no sentido que suas organizações acompanham com eficácia os custos relativos às atividades de cumprimento, e nesse aspecto estão bem à frente de seus colegas de outras regiões. Finalmente, 74% dos CEOs da América do Sul estão convencidos de que as atividades de cumprimento reduzem significativamente ou eliminam os riscos de não cumprimento, mais uma vez colocando-se na dianteira em relação a outras regiões do mundo.

Cerca de 70% dos CEOs da América do Sul, da Europa e da Ásia afirmaram dispor das informações necessárias para gerir o risco no âmbito da empresa como um todo – visão compartilhada por uma maioria menor de CEOs dos EUA (57%).

Em resumo, os CEOs da América do Sul, da Europa e da Ásia relatam elevados níveis semelhantes de gestão de riscos e confiança no sistema de controles internos.

Vale ressaltar que os CEOs dos EUA, em geral, possuem mais incentivos a assumir riscos do que os CEOs das demais áreas, uma vez que a remuneração desses executivos é mais atrelada a performance das ações no mercado de capitais das companhias geridas pelos mesmos. Desta forma, esses executivos por serem

“tomadores de risco” possuem uma percepção diferente no que tange a segurança dos controles.

Neste contexto, é fundamental que as opiniões dos CEOs, além de corretas, estejam baseadas em avaliações bem fundamentadas dos seus respectivos sistemas de controles.

O papel dos responsáveis por avaliar esses sistemas de controles das instituições financeiras passa a ser relevante, no sentido de avaliar adequadamente os riscos existentes nas organizações e de verificar a eficiência e eficácia dos controles internos. Para isso é necessário avançar no assessoramento à Alta Administração, modernizando-se, participando mais ativamente do planejamento estratégico, da avaliação do risco de suas carteiras de ativos, do estabelecimento de pontos de controle quando do lançamento de novos produtos e serviços, e de propor melhorias capazes de otimizar os resultados e de agregar valor, reduzindo, conseqüentemente, as perdas.

## 1.5 – Estrutura da Dissertação

A estrutura geral da dissertação está dividida em 12 capítulos. O capítulo introdutório procurou justificar a escolha do tema, incluindo os principais motivadores, e os principais objetivos da dissertação.

No capítulo dois é apresentada a revisão bibliográfica da pesquisa, com a caracterização dos sistemas de controles internos, suas origens e tendências, incluindo a apresentação dos fundamentos das principais metodologias de gestão dos controles internos.

No capítulo três é explorada a metodologia comumente utilizada no processo de avaliação dos controles internos, descrevendo de forma genérica cada uma das etapas necessárias no processo, desde o planejamento até a emissão do produto final.

Do capítulo quatro até o capítulo onze, são abordados os principais riscos inerentes às instituições financeiras com foco nas operações de tesouraria, focando nos principais controles para gestão dos respectivos riscos, sendo o principal objetivo da dissertação sugerir aos responsáveis pela avaliação desses controles, os testes que devem ser realizados para avaliar a eficiência e eficácia do sistema de controles internos.

Finalmente, no capítulo doze são apresentadas as conclusões sobre a importância da gestão dos controles internos para a sobrevivência das instituições

financeiras e dos demais agentes econômicos, incluindo acionistas, credores, clientes e outras instituições financeiras.

## 2- Controles Internos em instituições financeiras

### 2.1- Introdução

Ao desempenhar a sua função básica, que é reduzir a probabilidade de perdas financeiras, o sistema de controles internos está, na verdade, preocupado em gerir os riscos das instituições. Ao longo dos anos, o conceito de gerenciamento de risco vem se ampliando.

Urge ressaltar os conceitos de riscos operacionais definidos pelo Comitê da Basiléia, segundo o qual o risco operacional é definido como o risco de perda resultante de pessoas, sistemas e processos internos inadequados ou deficientes, ou de eventos externos.

Sem dúvida, na avaliação dos controles internos é fundamental estar atento aos riscos crédito, mercado e demais riscos, contudo, a gestão desses riscos começa pela gestão dos processos, pessoas, sistemas e fatores externos. Portanto, somente reduzindo esses riscos operacionais é possível reduzir os demais riscos e é nessa premissa que deve ser feita a avaliação dos sistemas de controles internos.

Internacionalmente, desde os primórdios dos anos 70 com a criação do Comitê da Basiléia para Supervisão Bancária, procurou-se fortalecer o Sistema Financeiro através da maior regulamentação sistemática de suas atividades, parametrizando-as pelas boas práticas financeiras e munindo-as de procedimentos prudenciais na sua atuação.

Duarte e Lelis (2002) mencionam que o principal objetivo do Acordo de Capital emitido pelo Comitê da Basiléia em 1998, o qual propunha um conjunto mínimo de diretrizes para o cálculo de adequação de capital, foi fortalecer a solidez e a estabilidade do sistema bancário pela recomendação da constituição de um capital mínimo por parte dos bancos, de forma a minimizar os riscos de insolvência das atividades bancárias.

Em paralelo a este cenário, as instituições financeiras brasileiras continuaram a enfrentar uma acirrada disputa interna por uma fatia cada vez mais representativa do mercado. Esta competitividade contribuiu para a quebra de algumas instituições que, dentre outros fatores, não adequaram seus Controles e não praticaram os Princípios Éticos.

Recentemente outros fatos relevantes no cenário mundial, tais como o ato terrorista nos EUA em 2001 e os escândalos financeiros em Wall Street em 2002, despertaram para a necessidade de regulamentações ainda mais efetivas e rapidamente aplicáveis em todos os países, buscando gerir os riscos aos quais as instituições estão sujeitas.

Com isso, as instituições financeiras foram compelidas a iniciar um ciclo de mudanças cada vez mais radicais, com reestruturações estratégicas, organizacionais e tecnológicas, além de reciclagens constantes buscando uma otimização do recurso humano, por meio de treinamentos periódicos e da implementação de ferramentas de controles internos.

Buscou-se a construção de uma imagem forte da instituição financeira junto a clientes e fornecedores, alinhando todo o conjunto de informações em eficazes meios de comunicação e processos internos, de modo a facilitar o acesso de colaboradores às informações institucionais, transformando-os em membros comprometidos e efetivos na busca de melhores resultados.

Os gestores que formam os pilares da Governança Corporativa, chegam ao momento em que todas estas transformações ocorrem simultaneamente e por isso suas implementações nas Instituições Financeiras Brasileiras tem importância e missão maior que aquela implícita na Resolução n.º 2554/98, uma vez que estas mudanças visam alinhar seus processos, assegurar o cumprimento das normas e procedimentos, e principalmente, preservar sua imagem perante o Mercado.

A Resolução 2.554/98 do Bacen estabelece que os controles internos, independentemente do porte da instituição, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas, e o acompanhamento sistemático das atividades relacionadas com o sistema de controles internos deve ser objeto de relatórios, no mínimo semestrais.

Neste contexto, o mercado brasileiro seguiu os moldes do americano, criando um novo departamento dentro das instituições, denominado Compliance, que seria responsável por estabelecer os controles necessários para atender a legislação e fortalecer os controles.

O Grupo de Trabalho ABBI/Febraban (2004) ressaltada que as atividades de Compliance podem ser entendidas como uma necessidade decorrente de fatos como demonstrado no Anexo 3. Urge ressaltar, a diferença entre Auditoria Interna e Compliance segundo o Grupo de Trabalho ABBI/Febraban em que “As atividades desenvolvidas por estas áreas não são idênticas, mas sim complementares, pois enquanto a Auditoria Interna efetua seus trabalhos de forma aleatória e temporal, por meio de amostragens, a fim de certificar o cumprimento das normas e processos instituídos pela Alta Administração, o Compliance executa suas atividades de forma rotineira e permanente, sendo responsável por monitorar e assegurar de maneira corporativa e tempestiva que as diversas unidades da Instituição estejam respeitando as regras aplicáveis a cada negócio, por meio do cumprimento das normas, dos processos internos, da prevenção e do controle de riscos envolvidos em cada atividade.”.

Recentemente, vem ganhando força nas instituições financeiras de grande porte, o conceito de um departamento de gestão de risco operacional que estaria focado nas perdas operacionais e na respectiva gestão dos riscos operacionais, incluindo a modelagem dos mesmos.

Ressaltamos que, com a criação de diversos departamentos que estariam diretamente responsáveis por gerir os riscos operacionais e seus respectivos controles, é necessário que as atribuições sejam bem definidas, evitando a sobreposição de tarefas que poderiam resultar em batalhas potenciais por território e uma relutância das áreas em trabalharem em conjunto.

Uma eficiente Gestão Corporativa deve basear-se numa análise criteriosa da adequação dos processos e da cultura e disciplina organizacional, recursos humanos e tecnologia, na aplicação de controles rigorosos do gerenciamento dos Riscos, devendo abranger ainda uma determinada e constante atuação em conjunto com as demais áreas, na busca de controles preventivos e detectivos.

## 2.2- Controles internos

Magliavacca (2002) define controle interno como o "planejamento organizacional e todos os métodos e procedimentos adotados dentro de uma empresa, a fim de salvaguardar seus ativos, verificar a adequação e o suporte dos dados contábeis, promoverem a eficiência operacional e encorajar a aderência às políticas definidas pela direção".

Segundo D´Avila (2002), "controle interno é um processo executado pelo conselho de administração, gerência e outras pessoas de uma organização, desenhado para fornecer segurança razoável sobre o alcance dos objetivos de eficiência e eficácia operacional; mensuração de desempenho e divulgação financeira; proteção de ativos; e cumprimento de leis e regulamentações.".

Conforme Andrade (1999), "controle interno compreende o plano organizacional e todos os procedimentos, métodos e medidas adotados pela empresa para: proteger seu patrimônio; assegurar a fidedignidade da informação utilizada para o processo decisório, gerencial e de controle; contribuir para estimular a eficiência

operacional; e incentivar a observar as políticas e diretrizes estabelecidas pela direção.”.

O conceito de controles internos foi extensamente discutido também por órgãos no Brasil e no exterior e a teoria do controle interno submeteu-se a diversas mudanças durante a última década. Estas mudanças começaram em 1988, quando o American Institute of Certified Public Accountants (AICPA) emitiu o *Statement on Auditing Standard* (SAS) no. 55, descrevendo o controle interno no âmbito de três componentes principais: controle do ambiente, o sistema de contabilidade, e os procedimentos do controle. Quatro anos mais tarde, o *Committee of Sponsoring Organizations* (COSO) emitiu um documento denominado *Internal Control: Integrated Framework*, caracterizando o controle interno como cinco componentes chaves: controle do ambiente, as atividades do controle, a avaliação de risco, a informação e a comunicação, e a monitoração.

Posteriormente, em 1995, a AICPA adotou os cinco componentes do COSO na definição dos controles interno e emitiu o SAS no. 78 para suplementar SAS no. 55.

O *Institute of Internal Auditors* (IIA) emitiu o relatório de *System Auditability and Control Report – SAC* em 1991, fornecendo a orientação do controle interno no âmbito de tecnologia de informação (TI), propondo uma estrutura para a discussão dos riscos, dos procedimentos do controle, e das considerações do exame relacionadas a TI. Finalmente, em 1995, o *Information System Audit and Control Association* (ISACA), publica uma coleção dos materiais chamados *CobiT Audit Guidelines*,

revisado em 1998. O *CobiT Audit Guidelines* fornece uma estrutura para os objetivos do controle e da avaliação em sistemas e em tecnologias de informação.

Moreira (2003) menciona que a Resolução 2.554 do Banco Central do Brasil, de 24 de setembro de 1998, introduziu o conceito de controles internos nas instituições financeiras no Brasil. Ainda segundo o autor, a legislação inaugura uma nova fase no Banco Central do Brasil, por meio de um sistema de audiências públicas, visando ao recebimento de sugestões do público em geral, objetivando a edição de normas mais condizentes com a realidade e a expectativa da sociedade, sob a visão de que a transparência é fundamental para o alcance da credibilidade.

Dado estes vários pronunciamentos sobre controle interno pelas organizações profissionais, faremos uma síntese das interpretações principais do conceito do controle interno.

### 2.2.1- COSO: *Internal Control: Integrated Framework*

Conforme Barbosa (1999), em 1942, o *American Institute of Certified Public Accountants, Institute of Internal Auditors, American Accounting Association, Institute of Management Accountants e Financial Executives Institute*, em conjunto, desenvolveram trabalho intitulado *Internal Control – Integrated Framework.*

O COSO *Internal Control: Integrated Framework* define o controle interno como um processo, efetuado pela diretoria, gerência e demais funcionários,

projetando fornecer a garantia razoável a respeito da realização dos objetivos nas seguintes categorias:

- Eficácia e eficiência das operações.
- Confiabilidade do relatório financeiro.
- Compliance com leis e regulamentos aplicáveis.

Esta definição foca diversos conceitos chaves tais como o "processo," "garantia razoável," e os "objetivos" do controle interno. O controle interno é um processo porque deve ser planejado, executado, e monitorado pelos diretores e gerentes de uma entidade e porque é a soma de uma série de ações integrantes dos processos do negócio de uma entidade.

O controle interno pode somente fornecer razoável, mas não absoluta, garantia a respeito da realização dos objetivos de uma entidade. Os objetivos de uma entidade para o controle interno incluem não somente a confiabilidade do relatório e compliance financeiros com leis e regulamentos aplicáveis, mas também a eficácia e a eficiência das operações.

A metodologia COSO possui cinco componentes que se relacionam entre si:

- Ambiente de Controle

Correspondendo a base que norteia os demais componentes. Está relacionado a fatores como ética, integridade, forma de conduta, políticas de recursos humanos, estrutura da organização, forma de atuação e atenção da Alta administração quanto à cultura de

controle, designação adequada de autoridade e responsabilidade e alocação adequada de recursos.

- Avaliação de Risco

Corresponde à identificação e análise de risco que são relevantes para os objetivos da empresa. Esta avaliação deve considerar a sua severidade, freqüência com que estes ocorrem e o grau de impacto.

- Atividade de controle

Referente às políticas e procedimentos que asseguram que os planos e direcionamento indicados pela administração são atingidos e ocorrem através de toda organização, em todos os níveis e funções, inclusive segurança física e lógica.

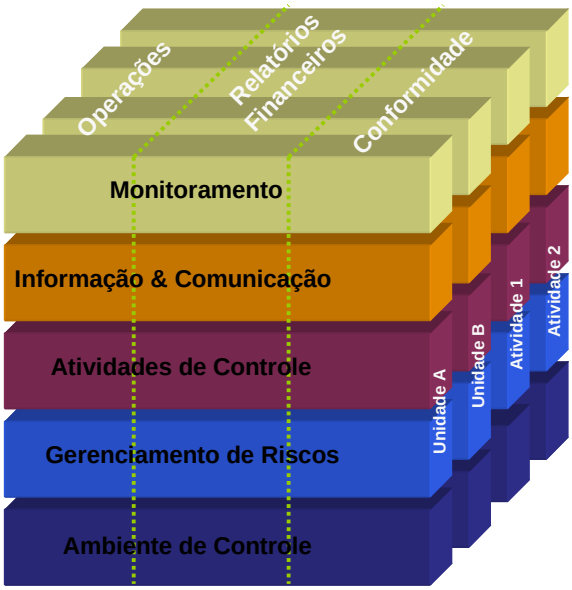
- Informação e comunicação

Corresponde à parte referente à emissão de relatórios operacionais, financeiros e de conformidade que possibilita o gerenciamento do negócio. Além disso, é o mecanismo de fluxo de comunicação através de toda organização em todos os níveis hierárquicos e com órgãos externos.

- Monitoramento

Processo de verificação e aperfeiçoamento contínuo das operações, incluindo a identificação das deficiências e encaminhamento aos responsáveis para correção das falhas.

Figura 1: Estrutura tridimensional integrada do Coso




Fonte: *Committee of Sponsoring Organizations of the Treadway Commission*

A eficiência do sistema de controles internos engloba a presença e o correto funcionamento de cada um dos cinco componentes em relação a cada um dos três objetivos do negócio: eficácia e eficiência das operações, confiabilidade do relatório financeiro e compliance com leis e regulamentos aplicáveis.

### 2.2.2- SAS 55/78 – *Statement on Auditing Standard*

Conforme citado pelo CRC SP (1998), o AICPA definiu controle interno como plano da organização e todos os métodos e medidas coordenados, adotados dentro da empresa para salvaguardar seus ativos, verificar a adequação e confiabilidade de seus dados contábeis, promover a eficiência operacional e fomentar o respeito e obediência às políticas administrativas fixadas pela gestão.

Em outubro de 1958, através do SAS (*Statement on Auditing Standards*) nº. 29 – *Internal Control*, procurou esboçar uma segregação entre as funções contábeis e administrativas, englobadas no sentido amplo de controles internos que anteriormente havia definido, e que já reconhecera sendo uma definição abrangente.

Posteriormente, foram emitidos os SAS nº. 78 e nº. 55. O SAS no. 78 alterou o SAS nº. 55 substituindo suas definição e descrição da estrutura interna do controle com aquela prescrita no relatório do COSO. O COSO tende a referir-se a todos os sistemas de informação, tanto operacional quanto financeiro, ao passo que o SAS no. 78 enfatiza somente aqueles sistemas e controles relevantes aos objetivos de relatório financeiros. Basicamente, o SAS no. 78 adota a definição dos cinco componentes do COSO, expandindo a definição e substituindo elementos do SAS no. 55. Os cinco componentes do COSO - controle do ambiente, a informação e a comunicação, as atividades do controle, a avaliação de risco, e o monitoramento dão uma compreensão maior àquelas que tentam fazer operacionais os conceitos em um sistema eficaz.

Os dois componentes novos do SAS no. 78 são a avaliação e monitoramento de risco. A avaliação de risco no SAS no. 78 refere-se ao processo da organização de identificar riscos potenciais para atingir seus objetivos de relatórios financeiros, visto que a definição do COSO incentiva a utilização de mecanismos para identificar, analisar, e controlar os riscos relacionados aos setores de vendas, produção, marketing, financeiros, e outras atividades.

### 2.2.3 - *Systems Auditability Control Report (SAC)*

O relatório do SAC define o controle interno como meios de fornecer a garantia razoável que os objetivos da organização são alcançados de uma maneira eficiente, eficaz, e econômica. O sistema do controle interno é descrito como um jogo dos processos, funções, atividades, subsistemas, procedimentos, e a organização de recursos humanos que fornece a garantia razoável que os objetivos da organização serão atingidos e o risco é aceitável.

Apesar desta definição ampla, o relatório próprio do SAC trata somente dos objetivos impactados pelos sistemas de informação da organização. Estes incluem a integridade da informação usada para finalidades da tomada de decisão, a segurança e a proteção da organização recursos, e o compliance com procedimentos e regulamentos internos e externos.

O SAC compartilha dos conceitos chaves do "processo," "garantia razoável," e "objetivos" com o relatório do COSO , embora sua estrutura tenha elementos em comum com o SAS no. 55 no que tange seus componentes dos sistemas do ambiente do controle.

O ambiente do controle inclui a estrutura de organização, a estrutura do controle, as políticas e os procedimentos da organização, e influências externas. Os sistemas manuais e automatizados incluem todas as maneiras em que a informação do negócio de uma organização é processada, relatada, armazenada, ou transferida. A avaliação de risco e o monitoramento são discutidas extensivamente no relatório, mas

não definidas explicitamente. Assim, o relatório do SAC é muito similar ao COSO, com o foco primeiramente na informação, e de forma secundária na vantagem do competidor organizacional.

### 2.2.4- *Control Objectives for Information and related Technology* (CobiT)

O CobiT é um produto das associações Cobit Steering Committee e do Information Systems Audit and Control Association - ISACA e busca reduzir as diferenças existentes entre os modelos de controle dos negócios e um modelo de controle mais focado em TI.

O CobiT fornece dois conceitos básicos de controle: controle e controle de TI. O conceito do controle é adaptado do relatório do COSO e definido como "as políticas, os procedimentos, as práticas, e as estruturas organizacional projetadas para fornecer a garantia razoável que os objetivos de negócio serão atingidos e que os eventos indesejados serão mitigados ou detectados e corrigidos." Essa definição torna a definição de "controle" do CobiT equivalente à definição de "controle interno” do COSO.

Entretanto, os objetivos do controle do CobiT são definidos de uma maneira orientada no processo. O conceito de “controle de TI" é adaptado do relatório do SAC e definido como "uma indicação dos resultados ou da finalidade desejada, executando procedimentos do controle em um detalhe da atividade de TI.”.

O domínio do CobiT consiste em quatro partes: planejamento e organização, aquisição e execução, entrega e sustentação, e monitoramento. Os processos, 34 ao todo, são identificados dentro de cada um dos quatro domínios. Conseqüentemente, as atividades da rotina de TI dentro dos processos são identificadas.

O objetivo central do controle é conectar os domínios, processos, e atividades de TI aos processos operacionais e às atividades da entidade. Objetivo que deve basicamente facilitar a realização dos objetivos do negócio. Os objetivos do negócio são consultados a como de "exigências do negócio para a informação" e incluem o seguinte:

- Exigências de qualidade (qualidade, custo, e entrega).
- Exigências fiduciárias, como definidas por COSO (eficácia e eficiência das operações, da confiabilidade da informação, e do compliance com leis e regulamentos).
- Exigências da segurança (confidencialidade, integridade, e disponibilidade).

### 2.2.5- Considerações

Inicialmente, todos os objetivos dos controles, independente da metodologia, são preocupações da Gerência. Em particular, a Alta Administração deve monitorar os controles que garantem as vantagens competitivas em relação à eficiência e eficácia operacional e disponibilização de produtos e serviços diferenciados.

Conforme demonstrado, o sistema de controles internos não deve se restringir às demonstrações contábeis e financeiras, abrangendo toda organização e sua respectiva operação. Por isso, deve estar atento aos controles executados por todos os funcionários, independente de sua posição hierárquica, sabendo que o maior risco a ser mitigado é o fracasso da instituição.

Tabela 2: Comparação das metodologias de controles internos

| | Cobit | SAC | Coso | SASs 55/78 |
|---|---|---|---|---|
| Usuário Primário | Alta Administração, usuários e auditores de sistemas | Auditores Internos | Gerência | Auditores Externos |
| Definição de Controles Internos | Conjunto de processos, incluindo políticas, procedimentos, práticas e estruturas organizacionais. | Conjunto de processos, subsistemas e pessoas | Processo | Processo |
| Objetivos | Eficácia e eficiência operacional, confidencialidade, integridade e disponibilidade de demonstrações financeiras confiáveis. Compliance com leis e regulamentos | Eficácia e eficiência operacional e Compliance com leis e regulamentos | Eficácia e eficiência operacional e Compliance com leis e regulamentos | Disponibilidade de demonstrações financeiras confiáveis, Eficácia e eficiência operacional e Compliance com leis e regulamentos |
| Componentes da Estrutura de Controle | Domínios: Planejamento e Organização; Aquisição e Implementação; Entrega e Sustentação de monitoramento | Componentes: Ambiente de controle; Sistemas Manuais & Automáticos; Procedimentos de Controle. | Componentes: Ambiente de controle; Gerenciamento de riscos; Atividades de Controle; Informação e Comunicação e Monitoramento | Componentes: Ambiente de controle; Gerenciamento de riscos; Atividades de Controle; Informação e Comunicação e Monitoramento |
| Foco | Tecnologia da Informação | Tecnologia da Informação | Organização como um todo | Demonstrativos Financeiros |
| Avaliação de controles internos | Por um período de tempo | Por um período de tempo | Em uma determinada data | Por um período de tempo |
| Responsabilidade pelos controles internos | Alta Administração | Alta Administração | Alta Administração | Alta Administração |
| Tamanho | 187 páginas em 4 documentos | 1193 páginas in 12 módulos | 353 páginas em 4 volumes | 63 páginas em 2 documentos |
| | | | | |

Fonte: Information Systems Audit and Control Association

Todos os funcionários na organização são efetivamente responsáveis pela eficiência e eficácia dos controles internos, cabendo à Alta Administração fazer com que esta sintonia esteja adequada. Contudo, alguns departamentos possuem um papel de destaque dentro do processo. São os chamados gestores dos controles internos que, dependendo da instituição, suas atribuições geralmente ficam nas áreas de Controladoria, Controles Internos, Compliance, Auditoria Interna, entre outros.

Os gestores dos controles internos são responsáveis por avaliarem os controles, sugerir melhorias, implementar políticas e procedimentos e auxiliar a Alta Administração no monitoramento dos controles internos.

Com as exigências dos órgãos reguladores, no Brasil definido especialmente a partir da emissão da Resolução 2.554/98, a partir de 1999, as instituições financeiras foram obrigadas a criar suas estruturas específicas para efetuar controles de forma eficaz.

## 3- Metodologia

O processo de avaliação do sistema de controles internos pode ser divido nas seguintes fases:

- Definição do escopo
- Entendimento do negócio
- Identificação dos riscos
- Elaboração de programa de trabalho
- Execução dos testes
- Emissão de relatórios

O processo de avaliação dos controles internos segue o procedimento básico de um processo tradicional de auditoria. Contudo, a maior contribuição da pesquisa estará na identificação e sugestão de testes dos controles dos riscos operacionais existentes.

Apesar da extensa literatura teórica sobre identificação e modelagem do risco operacional, pouco foi realmente publicado sobre as situações práticas existentes e que, muitas vezes, é comum às diversas instituições financeiras.

Neste contexto, será descrito todas as etapas do processo de avaliação dos controles internos. Contudo, o foco da dissertação será a apresentação dos principais riscos e a respectivas sugestões de testes para a verificação da eficiência e eficácia dos controles internos na gestão dos principais riscos inerentes às instituições financeiras.

## 3.1- Definição do Escopo

A avaliação do sistema de controles internos em uma instituição financeira de grande porte pode ser intimidador. O processo requer o suporte de um grande número de pessoas e uma relativa multiplicidade de fontes de dados, técnicas de análises e opções gerenciais.

A primeira etapa do processo consiste na definição do escopo do programa. Em Marshall (2002), é ressaltada a adoção das seguintes recomendações:

***Otimização***

O foco deve ser nos processos e recursos mais críticos, ou seja, onde estariam as maiores probabilidades de perdas, buscando, inclusive, o Princípio de Pareto – a maior parte (cerca de 80 por cento) do risco advém de um pequeno número (cerca de 20 por cento) de eventos de perda. Avaliar diversos riscos pode ser complexo demais e acabar perdendo o objetivo do projeto.

***Transparência***

O ideal seria desenvolver os primeiros passos em locais de negócio junto a gerentes operacionais amigáveis e apoiadores. É, portanto, essencial que esses gerentes compreendam os objetivos do projeto e como ele afetará seus negócios diários. Somente desta forma, é possível obter as melhores informações.

***Envolvimento da Alta Administração***

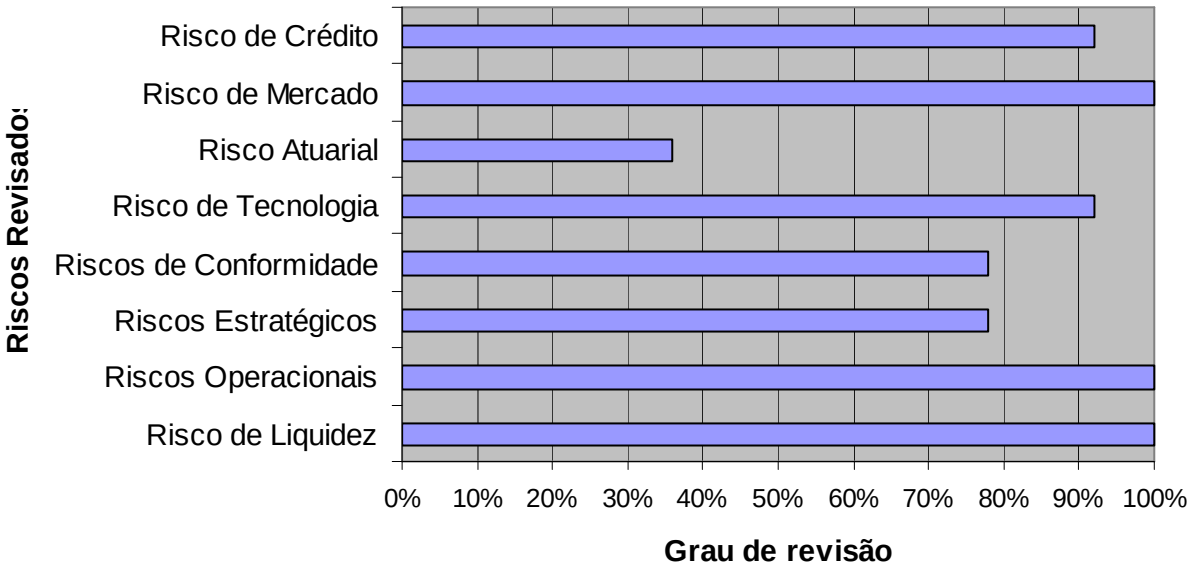
Em última instância, o resultado final das análises são recomendações de melhoria nos controles que precisariam sem implementadas nas próprias linhas de negócio e, portanto, o apoio da Alta Administração é essencial.

Adicionalmente, o envolvimento da Alta Administração pode ser eficaz para a identificação dos maiores riscos.

***Flexibilidade***

O acesso as diversas pessoas pode ser difícil e esporádico. É importante antecipar-se aos problemas e *deadlines* dos gerentes operacionais, tais como, fechamento de balanço ou reuniões de Comitês.

Tabela 3: Foco de atuação da Auditoria Interna na revisão dos riscos de tesouraria




Fonte: Febraban (2005b)

## 3.2- Entendimento do negócio

- **Mapeamento dos processos**

A identificação de risco deve ser sempre precedida da descrição e análise dos processos e controles. Marshall (2002) menciona os seguintes benefícios de estabelecer uma descrição formal dos processos da empresa:

Melhorar a compreensão da empresa do funcionamento de seus próprios processos. O mapeamento das combinações dos processos explica exatamente como suas ações afetam outras e onde se encontram as verdadeiras fontes de muitos problemas do dia-a-dia.

Melhorar a eficiência através da reengenharia e da redefinição do processo. O mapeamento de processos é um preâmbulo ao processo de reengenharia. Ele pode ser usado para desenvolver uma compreensão das atividades que adicionam valor aumentando o retorno ou diminuindo os riscos e das que não o fazem.

Ajudar a compreender a transferência de risco dentro da organização e ajudar a projetar as estratégias de apreçamento de risco. Os riscos tendem a ser transferidos em seqüência, de uma parte do processo para outra. O mapeamento de processos pode ser usado para alocar riscos de volta ao iniciador ou ao gerente de risco.

Ajudar a ditar uma abordagem sistemática ao planejamento de contingência através do mapeamento de recursos e processos. A falta de documentação aumenta

drasticamente o risco de que o processo não seja capaz de funcionar. O objetivo básico do planejamento de desastres é permitir que cada processo continue, ou seja, reiniciado se interrompido. Com o planejamento de catástrofe, o objetivo mais importante é recuperar o funcionamento total da organização tão rapidamente quanto possível, focando a atenção naqueles processos que não podem ser adiados para que a organização sobreviva.

Na prática, o mapeamento dos processos ocorre através de entrevista com o staff, avaliação das funcionalidades dos sistemas operacionais envolvidos, observação das rotinas, entre outros.

A formalização das conclusões e análise pode ser basicamente descritiva, através de memorando, ou com a fluxogramação utilizando softwares específicos, tal como, flowcharter.

O objetivo é reduzir o risco de falhas de comunicação e conseqüentes erros de entendimento por parte do avaliador. Desta forma, com a formalização dos conceitos, é possível certificar-se com os entrevistados ou mesmo com os demais membros da equipe de que o entendimento do processo foi bem assimilado.

A seguir apresentaremos a estrutura básica de uma instituição financeira e respectivos processos existentes em cada área:

**a) Tesouraria**

A tesouraria é uma área estratégica em qualquer instituição financeira. A área é normalmente responsável pela gestão financeira da carteira da instituição, desenvolvimento de negócios com empresas financeiras e não financeiras e investidores institucionais, desenvolvimento de novos produtos e controle da liquidez e dos fluxos de caixa da instituição financeira.

Segundo Duarte e Moreira (2005), a tesouraria é uma área que merece especial atenção em qualquer banco. De suas funções clássicas de captação e aplicação de recursos, passando por administração de fluxos, prazos, concentrações, descasamentos em moedas e taxas, além do apreçamento e das realizações para clientes, dependem, significativamente, a liquidez da instituição.

Moreira (2002) ressalta que uma área que tem demandado especial atenção em uma inspeção global consolidada realizada pelo Banco Central do Brasil é a tesouraria do conglomerado sob fiscalização. Em particular, a supervisão bancária tem dado especial atenção às operações em moeda estrangeira, às operações com títulos de dívidas, às operações com derivativos, aos instrumentos de gestão de riscos e aos controles internos voltados para a tesouraria.

Securato (2003) define que o ponto central das tesourarias consiste em captar e aplicar recursos, através de estratégias diversas de forma a obter ganhos.

O objetivo das tesourarias é obter um ponto ótimo entre um rígido controle do risco de mercado e liquidez vis-à-vis uma performance nos resultados que maximize a riqueza dos acionistas e clientes. A má gestão da tesouraria levando a falta de liquidez é a principal razão para o insucesso de uma instituição financeira.

A Tesouraria pode ser vista como um departamento segregado dos demais departamentos e subdividido conforme segue:

**Mesa de Moedas/Câmbio**

É na mesa de câmbio que são feitas as operações com moedas estrangeiras sendo que, no Brasil o dólar americano é a moeda mais negociada. Também são feitas as operações de dólar pronto, dólar financeiro e captações em moeda estrangeira (através de linhas e colocação de bônus, por exemplo)

**Mesa de Juros**

Aqui são feitas as operações de compra e venda de títulos de renda fixa dos tipos pré e pós fixados (CDI, CDB, NTN, LTN, LFT, Debênture, etc...) tanto no mercado primário quanto no mercado secundário. É também na mesa de juros que são feitas as captações em moeda doméstica, através da emissão de CDB´s, por exemplo.

**Mesa de derivativos**

Na mesa de derivativos são feitas as operações com contratos futuros de juros, de dólar, do índice e operações de FRA. Também são feitas as operações opções de juros, de dólar e do índice e as operações de swaps nas diversas taxas.

**Mesa de renda variável**

Na mesa de derivativos são feitas as operações tanto nas bolsas domésticas quanto nas bolsas internacionais, incluindo as negociações com ADRs. Muitas vazes é possível realizar operações de arbitragem com ações negociadas no Bovespa e os ADRs.

**Mesa Internacional**

Nesta mesa são realizadas operações com títulos de dívida externa de países emergentes, os Bradies, e títulos de outros países, como os títulos do governo americano, por exemplo. Também é nessa mesa que são feitas as transações de títulos privados (Corporate Bonds) emitidos no exterior por empresas domésticas ou estrangeiras, a exemplo dos Eurobonds.

**Research Macroeconômico**

A área de pesquisa macroeconômica é responsável pelas projeções dos indicadores macroeconômicos de forma a traçar cenários para o futuro, dando base para as operações da tesouraria e para as estratégias a serem adotadas.

**b) Alta Administração**

Responsável pela estratégia a ser tomada nas mesas de operações (câmbio, reais, derivativos, renda variável e internacional), pelo back-office e pela(s) área(s) de

gerenciamento dos riscos de crédito, mercado e liquidez, além da gerência do próprio risco operacional.

**c) Back-office**

O back office tem como função dar suporte as operações feita pelo front office, a área é responsável pelo processamento (confirmação e liquidação das transações) documentação (representa a parte legal do acordo entre os operadores) e os aspectos de controle das transações.

***c*) Middle office**

O middle office tem como função monitorar as operações feita pelo front office, sendo a área responsável pelo monitoramento independente dos riscos de mercado e liquidez da tesouraria.

Adicionalmente, essa área ocupa uma posição estratégia nas instituições financeiras, à medida que é responsável por prestar informações à Alta Administração, verificando de forma independente o cumprimento das políticas e estratégias pré-definidas pela Alta Administração.

Figura 2: Estrutura da Tesouraria

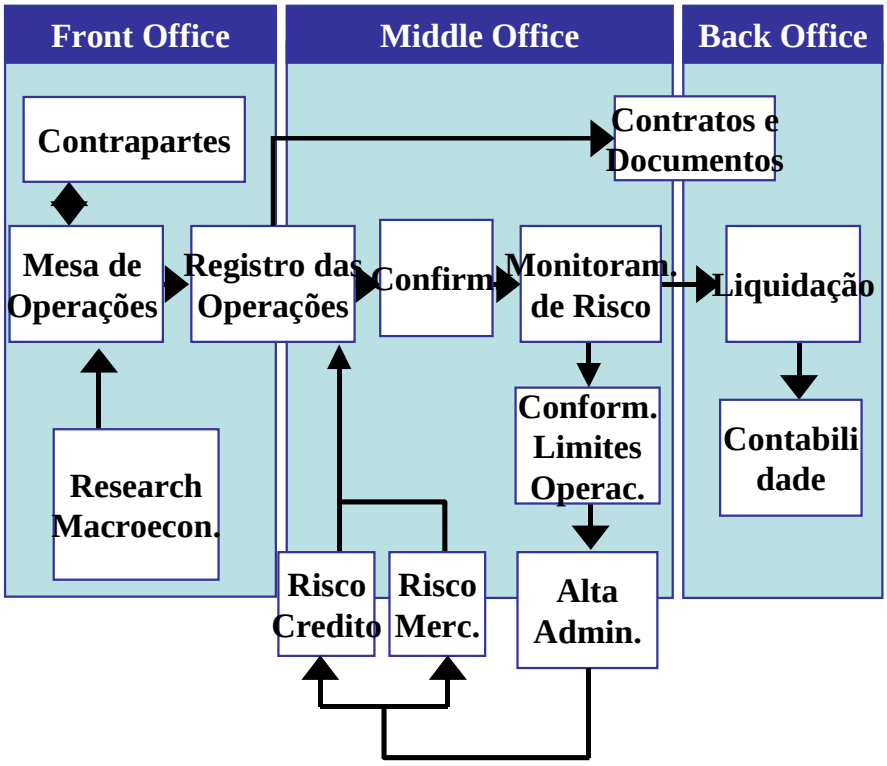


Tabela 4 – Resumo da estrutura de tesouraria

| Departamento | Funções e responsabilidades |
|---|---|
| Front Office | Análise de investimentos<br>Alocação de ativos<br>Negociação<br>Gerenciamento de portfolio |
| Middle Office | Gerenciamento de riscos<br>Cumprimento pré transacional<br>Relatório gerenciais<br>Fluxo de caixa<br>Monitoramento de limites e posições |
| Back office | Confirmação e liquidação<br>Valorização<br>Formalização<br>Contratos<br>Geração de informações para a contabilidade<br>“Reporte” local e matriz<br>Cumprimento da política de compras |

Fonte: Febraban (2005b)

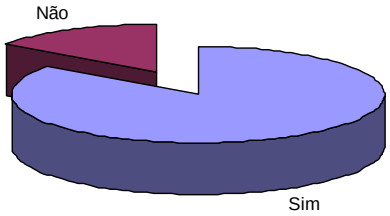
### 3.3- Identificação dos riscos

Após a identificação e mapeamentos dos processos operacionais críticos, o próximo passo é identificar os riscos que podem afetar o desempenho do processo e a utilização dos recursos. Realizar a identificação dos riscos nos processos requer, além do conhecimento do próprio processo, a participação dos gerentes de linha e supervisores graduados que têm a experiência do que pode dar errado no processo.

A identificação dos riscos é um processo interativo e está freqüentemente integrado ao planejamento estratégico. É importante considerar o processo também sob a forma da filosofia “clean sheet of paper”, ou seja, não considerar apenas os fatos ocorridos no passado.

Uma das ferramentas mais utilizadas em qualquer avaliação dos sistemas de controles internos seria uma matriz de risco ou dicionário de fatores de riscos precisamente definidos sob um aspecto macro e micro, de modo que todos na organização possam entender o significado do risco potencial. A simplicidade e padronização do dicionário facilitam o entendimento e disseminação de uma cultura de controle e transmissão rápida e eficiente dos problemas potenciais.

Figura 3: Utilização da Matriz de Riscos pelos Departamentos de Auditoria Interna




Fonte: Febraban (2005b)

Para identificação dos riscos, foi utilizado a Matriz de Riscos descrita proposta por Duarte (2005), que apresenta quatro principais grupos de riscos (Mercado, Operacionais, Crédito e Legais), classificados pelos tipos de fatores que geram a incerteza sobre cada um deles.

Tabela 5: Principais sub-áreas do risco de mercado

| Risco | Definição |
|---|---|
| Taxa de juros | Perdas potenciais devido a mudanças inesperadas nas taxas de juros |
| Taxa de câmbio | Perdas potenciais devido a mudanças inesperadas nas taxas de câmbio |
| Ações | Perdas potenciais devido a mudanças inesperadas nos preços das ações |
| *Commodities* | Perdas potenciais devido a mudanças inesperadas nos preços das *commodities* |
| Liquidez | Perdas potenciais devido ao fato de suas posições não poderem ser facilmente vendidas ou financiadas no mercado |
| Derivativos | Perdas potenciais devido ao uso de derivativos (para *hedge* ou especulação) |
| *Hedge* | Perdas potenciais devido ao mau uso de instrumentos de *hedge* |
| Concentração | Perdas potenciais devido a não diversificação da carteira |

Tabela 6: Principais sub-áreas do risco operacional

| Risco | Definição |
|---|---|
| Equipamentos | Perdas potenciais devido às falhas nos seus sistemas (telefônicos, elétricos, computacionais, etc..) |
| Obsolescência | Perdas potenciais devido à obsolescência de seus sistemas (de software, de hardware, telefônico, elétricos, etc...). |
| Confiabilidade e presteza | Perdas potenciais devido ao fato de as informações não serem recebidas, processadas, armazenadas e transmitidas com rapidez e de forma confiável. |
| Erro não intencional | Perdas potenciais devido a erros não intencionais (negligência falta de concentração no trabalho, falha de informação sobre os controles internos, etc..) |
| Fraudes, furtos e roubos | Perdas potenciais devido a fraudes, furtos ou roubos (negligência de controles internos, divulgação intencional de informações erradas aos clientes, manipulação de resultados, aceitação de 'incentivos'de clientes, etc..) |
| Qualificação | Perdas potenciais devido a funcionários sem qualificação apropriada |
| Produtos e serviços | Perdas potenciais devido ao não-atendimento, por produtos e serviços, das expectativas e necessidades de seus clientes, seja em produtos, seja em serviços. |
| Regulamentação | Perdas potenciais devido ao fato de a regulamentação externa ser alterada e não poder ser atendida pela firma |
| Liquidação financeira | Perdas potenciais devido a falhas nos procedimentos internos para liquidar transações |
| Modelagem | Perdas potenciais devido ao fato de os modelos matemáticos não serem adequadamente desenvolvidos e utilizados, e seus resultados, entendidos. |
| Imagem | Perdas potenciais devido à diminuição de reputação de mercado |
| Concentração | Perdas potenciais devido a negócios não adequadamente diversificados |
| Sistêmico | Perdas potenciais devido a alterações substanciais no ambiente operacional |
| Catástrofe | Perda potencial em função da instituição não poder operar devido à ocorrência de catástrofes (furacões, enchentes, terremotos, etc.). |

Tabela 7: Principais sub-áreas do risco de crédito

| Risco | Definição |
|---|---|
| Inadimplência | Perdas potenciais decorrente de uma contraparte não poderem fazer os pagamentos devidos de juros ou principal no vencimento destes |
| Degradação | Perdas potenciais devido à redução do *rating* de uma contraparte |
| Garantia | Perdas potenciais devido à redução do valor de mercado das garantias de um empréstimo |
| Soberano | Perdas potenciais decorrente de uma mudança na política nacional de um país que afete sua capacidade de honrar seus compromissos |
| Concentração | Perdas potenciais diante da concentração da exposição de crédito em poucas contrapartes |

Tabela 8: Principais sub-áreas do risco legal

| Risco | Definição |
|---|---|
| Legislação | Perdas potenciais devido a penalidades impostas por regulamentação ou processos de clientes contra a instituição |
| Tributário | Perdas potenciais decorrente da criação de novos tributos ou mudança na interpretação dos tributos existentes |
| Contrato | Perdas potenciais decorrentes de contratos omissos ou mal redigidos (sem o devido amparo legal) |

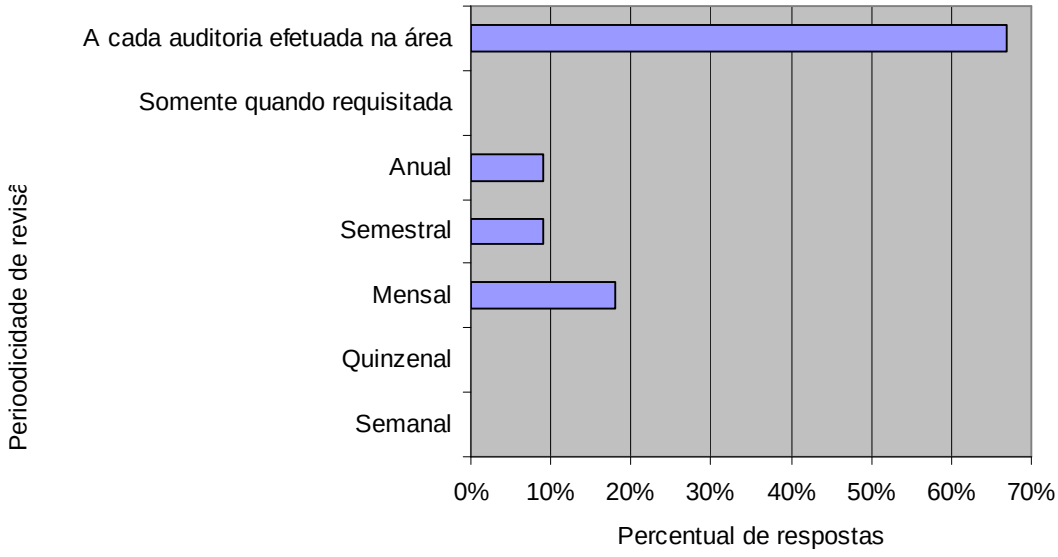
Contudo, a dissertação tem o objetivo de ressaltar os principais riscos que necessitam ser monitorados, especialmente os operacionais, sob um aspecto micro nas diferentes áreas da Tesouraria (Front, middle e back office).

.

### 3.4- Elaboração de programa de trabalho

Após o preenchimento da matriz de risco, serão elaborados os programas de trabalho para execução dos testes que visam definir a performance dos controles no que tange a mitigação dos riscos operacionais. Estes trabalhos devem ser executados na ordem de prioridade de cobertura de riscos determinada na Matriz de Risco, procurando-se aplicar a Rotação de Ênfase nos exames, a fim de otimizar a abrangência dos trabalhos. Menor rotação implica em cobertura de um período maior, através de um único exame, por exemplo: apenas 1 exame (menor rotação) num período de 3 anos; enquanto que maior rotação é obtida por maior número de exames, num determinado período. Dessa forma, a determinação da maior ou menor rotação de ênfase está relacionada com a relevância do risco.

Figura 4: Freqüência de avaliação pela Auditoria Interna dos controles



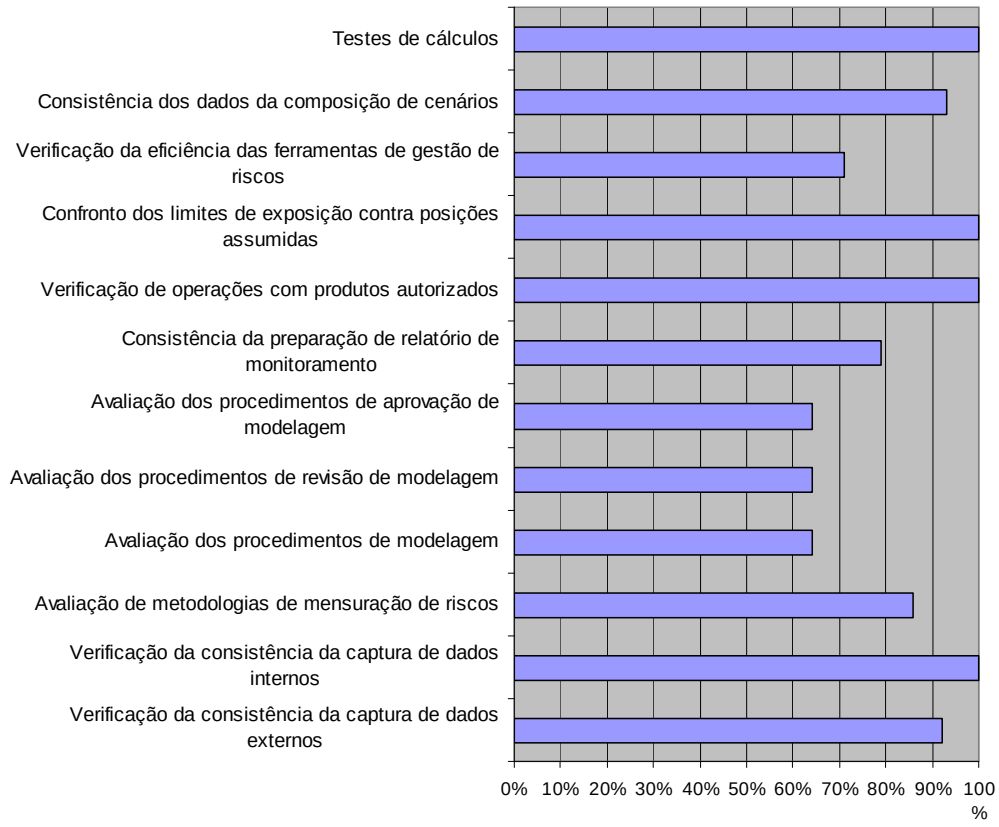

Fonte: Febraban (2005b)

Apesar da freqüência dos controles avaliados variarem, as fases são essencialmente as mesmas. No início do ano, os procedimentos operacionais e controles são revistos e avaliados para cada área; então através dos anos e dependendo da freqüência, um número de avaliações é reavaliado.

### 3.4- Execução dos testes dos controles

Os testes dos controles (ou de aderência, ou de procedimentos, ou de conformidade) servem para avaliar os cumprimentos das políticas e normas definidas pela Alta Administração. Com base no nível de conformidade verificado, é avaliado o grau de confiança que depositará nos controles internos, estendendo ou reduzindo os procedimentos dos testes a aplicar.

Figura 5: Procedimentos de revisão na área de tesouraria e gestão de riscos




Fonte: Febraban (2005b)

Esta fase é extremamente importante, pois é aqui que é feita à qualificação do sistema de controle interno e identificação de suas principais fragilidades. Alguns

sistemas são tão frágeis que incluem processos que não são “avaliáveis”, e é isto que deve ser deixar bem claro, negando-se a emitir opinião, ou, quando foram aplicados todos os procedimentos, emitir opinião negativa a respeito deste processo. Na maioria dos escândalos relacionados à fraude levados ao conhecimento público, esta situação existia e não foi observada, ou não se teve a independência, ou probidade, suficiente para assumir a obrigação e declarar que o sistema é “não avaliável”.

O custo de um controle não deve superar o benefício que este deverá gerar. Esta afirmação é uma constante em cartas de controle interno de auditores e relatórios gerenciais dos mais variados. Entretanto, um sistema de controle não-confiável impede a obtenção correta dos seus custos. Da mesma forma, os benefícios não podem ser avaliados, se o risco dos demais sistemas gerarem dados, igualmente, não-confiáveis.

Nesta fase, também, se avalia o grau de preocupação dos funcionários e gestores com os riscos inerentes ao seu processo. Processos críticos devem possuir controles adequados a fornecer respostas imediatas, permitindo monitoramento adequado de seu desempenho.

### 3.5- Emissão dos relatórios

O relatório de avaliação do sistema de controles internos deve ser elaborado à medida que concluído o trabalho e conterá todos os pontos julgados necessários.

O relatório deve possuir uma expressão inequívoca da conclusão do avaliador sobre a área auditada e seu conteúdo variará segundo a natureza e tamanho de cada projeto, mas deve conter tópicos como, por exemplo:

- tipo de exame;
- objetivos do exame;
- período examinado;
- princípios, normas e legislação aplicáveis;
- grau de cumprimento do programa de trabalho;
- principais mudanças operacionais, administrativas e financeiras ocorridas;
- resumos comparativos;
- problemas e questões que exigem estudo mais aprofundado;
- recomendações destinadas ao aprimoramento de sistemas e dos controles internos, especificando: falhas ou exceções identificadas, suas causas e conseqüências para os objetivos ou resultados da área/empresa/atividade; recomendação e benefícios que a mesma proporcionará; justificativa ou observações da área avaliada; efeito da deficiência; e datas em que as recomendações foram reportadas e corrigidas, ou serão corrigidas.

Adicionalmente, o Relatório deverá identificar o nível hierárquico ao qual é dirigido:

- recomendações à Alta Administração;
- recomendações destinadas ao aprimoramento das normas e procedimentos aos níveis gerenciais;

- recomendações para o cumprimento das normas existentes, aos níveis de execução.

O relatório terá características como, por exemplo:

- ser tão conciso quanto possível, mas ao mesmo tempo claro e completo, de modo que os usuários o entendam;
- ser organizado por área, departamento ou setor;
- manter uma estética uniforme de apresentação;
- apresentar a recomendação de forma sintética;
- identificar o objetivo da recomendação;
- exemplificar quando aplicável os desvios observados;
- apresentar opinião do encarregado da área encarregada, sobre a recomendação;
- inserir apenas informações baseadas em fatos documentados e conclusões devidamente fundamentadas por suficiente evidência nos papéis de trabalho.

## 4 - Avaliação do Ambiente de Informática

A gestão do ambiente de informática está associada basicamente à redução dos riscos de Equipamentos, Obsolescência, Confiabilidade e presteza, Fraudes, furtos ou roubos e Catástrofe.

À medida que a essência do negócio das instituições financeiras é a transação de valores monetários, adicionado ao fato que o registro e processamento das informações estão cada vez mais dependentes da tecnologia, as instituições financeiras estão extremamente suscetíveis a ataques e usos indevidos, especialmente as operações on-line tal como, as transações realizadas via Sistema de Pagamentos Brasileiro.

Oportunidades tornam-se vulnerabilidades, ao mero clique do mouse. O problema de segurança pode ser ampliado se a instituição financeira sofrer de falta de recursos e processos apropriados de proteção, dependendo de uma grande gama de tecnologias de segurança diferentes e intricadas.

O maior desafio consiste em desenvolver uma proteção escalonada, com boa relação custo-benefício e que permaneça um passo à frente das novas ameaças. Apesar do assunto “segurança na tecnologia da informação” ser bastante extenso e técnico, é necessário que as instituições financeiras possuam um Modelo de Gestão de Segurança da Informação.

Para os responsáveis por avaliar os controles internos, o maior desafio é avaliar o Modelo de Gestão da Segurança de Informação, considerando as diversas ameaças que podem ocasionar tipos diferentes de perdas, algumas significativas. Neste contexto, ressaltamos a utilização da metodologia Cobit como benchmarking neste modelo de gerenciamento do risco tecnológico, sendo uma das metodologias mais completas aplicáveis à área de TI. Esta metodologia é, inclusive, utilizada pelo Banco Central do Brasil nos trabalhos de revisão do ambiente de informática.

Devido a enorme variedade de arquiteturas de informação encontradas nas organizações contemporâneas, nenhuma metodologia de avaliação do ambiente tecnológico pode atender completamente a todos os tipos de ambientes a serem auditados. O grau de automação de rotinas físicas e intelectuais e de integração entre os sistemas, os tipos de tarefas e as decisões que os sistemas são projetados para assistir, a complexidade da organização – são muitos os aspectos que irão influenciar o processo de avaliação e fiscalização dos sistemas e da infra-estrutura de informação das organizações.

Apesar da complexidade e extensão dos assuntos, com base na metodologia Cobit, exploraremos os principais pontos de controles que devem ser avaliados na gestão do risco tecnológico.

## 4.1- Planejamento e Organização

### 4.1.1- Plano estratégico de TI

O primeiro passo é a definição de um plano estratégico de TI de alta qualidade, que cubra as perguntas básicas sobre o quê, quem, como, quando e por quê. O processo de planejamento de TI deve levar em consideração os resultados da avaliação de risco, inclusive os riscos do negócio, ambientais, tecnológicos e de recursos humanos.

Os aspectos que precisam ser levados em consideração e tratados de forma adequada pelo plano estratégico incluem:

- Abordagem e estrutura - alinhamento com a missão e estratégias corporativas da organização de curto e longo prazo, a distribuição geográfica, evolução tecnológica, custos, requisitos legais e regulamentares, requisitos de terceiros ou do mercado, horizonte de planejamento, re-engenharia do processo empresarial, designação de pessoal, distribuição do trabalho interna ou externamente, dados, aplicativos e arquiteturas de tecnologia. O objetivo é formalizar as vantagens das escolhas de forma clara e objetiva.
- Monitorar e avaliar - Os planos a longos e curtos prazos devem incorporar indicadores de desempenho e metas. Adicionalmente devem ser definidos processos para coletar e reportar feedback por parte dos proprietários de processos empresariais e usuários com relação à qualidade e utilidade de Planos a longo e a curto prazos.

- Controle das Mudanças no Plano de TI de Longo Prazo - Assegurar a existência de um processo para modificar o plano de TI de longo prazo de forma oportuna acomodando mudanças no plano à longo prazo da organização e mudanças nas condições de TI.
- Comunicação do plano - Assegurar que planos de TI a longo e a curtos prazos sejam comunicados a proprietários de processos empresariais e outras partes afetadas em toda a organização.
- Avaliação dos sistemas existentes - . Antes de desenvolver ou mudar o plano de TI estratégico ou a longo prazo, a administração de TI deve promover a avaliação dos sistemas existentes com relação à sua automação empresarial, funcionalidade, estabilidade, complexidade, custos e pontos fortes e fracos a fim de determinar o grau até onde os sistemas existentes comportam os requisitos empresariais da organização.

### 4.1.2- Definição de arquitetura das informações

Existência de um modelo de arquitetura de informação, abrangendo o modelo de dados corporativo e os sistemas de informação associados, ou seja, a instituição deve planejar como os dados e os sistemas se relacionarão, permitindo que as pessoas desempenhem suas responsabilidades com eficiência.

Como parte integrante do modelo, deve ser criado e atualizado continuamente um dicionário de dados corporativos que incorpore regras de sintaxe de dados da organização. Os referidos dados devem ser classificados em classes de informação, ou

seja, categorias de segurança, onde as regras de acessos dessas classes devem ser bem definidas.

### 4.1.3- Determinação da direção tecnológica

Deve ser assegurado pela área de TI que as tendências e condições regulamentares futuras possam ser levadas em consideração durante o desenvolvimento e a manutenção do plano de TI.

### 4.1.4- Definição da organização e as relações de TI

Deve existir uma estrutura de TI que garanta massa crítica, autoridade e independência dos usuários na estrutura geral da organização, até o ponto necessário para garantir soluções eficientes de TI e progresso suficiente em sua implementação com a finalidade de estabelecer uma relação de parceria com a alta administração com o objetivo de aumentar a conscientização, entendimento e habilidade de identificar e resolver questões relativas a TI.

Neste contexto, devem ser atribuídos papéis e responsabilidades com relação a sistema de informação, levando-se em conta a divisão apropriada de tarefas, onde nenhum indivíduo controla todos os aspectos principais de uma transação ou evento, e executa apenas aquelas tarefas estipuladas para sua respectiva área e cargo. Especificamente, deveria ser mantida uma divisão de tarefas entre as seguintes funções:

• uso de sistemas de informação

• inserção de dados

• operação de computadores

• gerenciamento de rede

• administração de sistemas

• desenvolvimento e manutenção de sistemas

• gerenciamento de alterações

• administração de segurança

• auditoria de segurança

Também devem ser definidos e implementado as políticas e procedimentos para controlar as atividades de consultores e outras pessoas contratadas pela área de TI para assegurar a proteção dos ativos relacionados a informações da organização.

### 4.1.5- Administração dos investimentos de TI

Deve existir um orçamento anual de operações de TI formalmente aprovado, respeitando os planos a longo e curto prazos da organização sendo, inclusive, investigadas alternativas para obtenção de financiamentos.

Adicionalmente, o referido orçamento deve comparar custos reais e previstos, relatar as vantagens advindas dos investimentos de TI, com a definição de indicadores de desempenho que possibilitem acompanhar os investimentos.

### 4.1.6 – Comunicação dos objetivos e direção da administração

É importante desenvolver políticas e estruturas que definam a abordagem geral da organização com relação à segurança e proteção dos recursos de TI e integridade dos sistemas de TI. As políticas devem advir das decisões da administração no tratamento de atividades, aplicativos, sistemas ou tecnologias específicos.

É parte integrante deste processo assegurar que essa política de segurança e de controles internos especifique o propósito e objetivos, a estrutura da administração, o escopo dentro da organização, a definição e atribuição de responsabilidades para implementação em todos os níveis e a definição de penas e ações disciplinares associadas à não-conformidade com as políticas de segurança e controles internos. A política deve estar em conformidade com os objetivos gerais do negócio e ser destinada a minimizar os riscos através de medidas preventivas, identificação oportuna de irregularidades, limitação de perdas e restauração oportuna. As medidas devem ser baseadas em análises de custo/benefício e devem ser priorizadas.

Adicionalmente, é recomendável a aplicação de uma política por escrito sobre os direitos de propriedade intelectual incluindo o software usado internamente.

O processo de comunicação deve ser inserido em um programa de conscientização de segurança em TI que deve comunicar as políticas de segurança de TI para cada usuário e assegurar um entendimento total da importância de tal segurança, cujo objetivo é transmitir a mensagem de que a segurança de TI está a favor da organização, de todos os seus funcionários e que todos são responsáveis por

ela. Esse programa de conscientização deveria ser apoiado pela administração e representar seu ponto de vista.

### 4.1.7- Cumprimento dos requisitos externos

Devem ser avaliadas as práticas organizacionais para garantir a conformidade com requisitos externos, atentando para a definição e manutenção de procedimentos adequados, assegurando conformidade contínua com, pelo menos, os seguintes fatores:

- Segurança e ergonomia - Assegurar conformidade com padrões de segurança e de ergonomia no ambiente de trabalho dos usuários e equipe de TI.
- Privacidade, Propriedade Intelectual e Fluxo de Dados - Assegurar conformidade com regulamentações sobre privacidade, propriedade intelectual, fluxo de dados e de criptografia aplicáveis às práticas de TI de uma organização.
- Comércio eletrônico - Assegurar que existam contratos formais definindo um acordo entre parceiros de negócios sobre processos de comunicação e sobre padrões para segurança das mensagens da transação e armazenagem de dados. Assegurar controles adequados para garantir a conformidade com leis e hábitos locais em uma base mundial, ao fazer negócios com parceiros no exterior.
- Conformidade com Contratos - Assegurar que os requisitos de contratos sejam identificados apropriadamente e constantemente satisfeitos.

### 4.1.8 – Gerenciamento dos projetos

Avaliar a estrutura geral de gestão de projetos assim como a metodologia de gerenciamento a ser adotada e aplicada a cada projeto. A metodologia deve abranger, pelo menos, a distribuição de responsabilidades, divisão de tarefas, planejamento de tempo e recursos, marcos, pontos de controle e aprovações.

Posteriormente, é importante assegurar o bom gerenciamento dos projetos com medidas como:

- Definição - criação de uma declaração por escrito definindo a natureza e o escopo de cada projeto de implementação antes do trabalho começar;
- Aprovação - a alta administração da organização deve revisar os relatórios dos estudos de viabilidade relevantes como base para sua decisão de como se proceder em cada projeto, propiciar que os gerentes designados das áreas de TI e os usuários aprovem o trabalho realizado em cada fase do ciclo antes que o trabalho da próxima fase se inicie;
- Aprovação da fase do projeto - Assegurar que para cada projeto aprovado seja criado um plano diretor adequado à manutenção de controle do projeto em toda a sua duração e que inclua um método de se monitorar o tempo e custos incorridos na duração do projeto;
- Plano Diretor - Assegurar que para cada projeto aprovado seja criado um plano diretor adequado à manutenção de controle do projeto em toda a sua duração e que inclua um método de se monitorar o tempo e custos incorridos na duração do projeto;

- Plano de Teste - Exigir a criação de um plano de teste para cada projeto de desenvolvimento, implementação e modificação.;
- Plano de Treinamento - Exigir a criação de um treinamento para cada projeto de desenvolvimento, implementação e modificação.
- Plano de Revisão - Oferecer, como parte integral das atividades da equipe do projeto, o desenvolvimento de um plano para a revisão da pós implementação de cada sistema de informação novo ou modificado para determinar se o projeto teve os benefícios planejados.

## 4.2 – Aquisição e implementação

### 4.2.1 - Identificação das Soluções Automatizadas

- Definição de requisitos de informação - Avaliar se os requisitos de negócios satisfeitos pelo sistema atual e a serem satisfeitos pelo sistema proposto novo ou modificado (software, dados e infra-estrutura), sejam claramente definidos antes que seja aprovado um projeto de desenvolvimento, implementação ou modificação. A metodologia de ciclo de vida de desenvolvimento de sistemas deve exigir que os requisitos operacionais e funcionais da solução sejam especificados, incluindo desempenho, proteção, confiabilidade, compatibilidade, segurança e legislação.

- Formulação de Estratégias de Aquisição - Avaliar plano de estratégia de aquisição de software definindo se o software será adquirido pronto para uso, desenvolvido internamente, adquirido através de contrato ou através de melhorias em software existente ou uma combinação desses fatores. A aquisição, desenvolvimento e manutenção de sistemas de informação devem ser considerados no contexto dos planos de TI a longo e a curto prazos da organização.

- Controles de Segurança com Boa Relação Custo-Benefício - Assegurar que os custos e benefícios de segurança sejam cuidadosamente examinados em termos monetários para garantir que os custos de controles não excedam suas vantagens. Devem ser definidos os requisitos de segurança para a gestão de continuidade de negócios para assegurar que os processos de ativação, fallback e retomada sejam

suportados pela solução proposta. A decisão requer aprovação formal da administração. Todos os requisitos de segurança devem ser identificados na fase apropriada do projeto e devem ser justificados, concordados e documentados como parte do processo de negócios no caso de um sistema de informação.

- Desenho das Trilhas de Auditoria - Exigir que estejam disponíveis ou que sejam desenvolvido mecanismos adequados para trilhas de auditoria para a solução identificada e selecionada. Os mecanismos devem oferecer a capacidade de proteger os dados sensíveis (por exemplo, identificações de usuários) contra mal-uso e incompatibilidade de funções.

- Controle de Obtenção de Produtos - Avaliação da abordagem, geralmente centralizada, para a obtenção de produtos com a descrição de um conjunto comum de procedimentos e padrões a serem seguidos na obtenção de hardware, software e serviços relacionados à Tecnologia da Informação.

- Programação de Aplicativo - Avaliar os controles sobre a obtenção de serviços de programação, atentando para formalização das justificativas através de uma solicitação por escrito de serviços de um determinado membro de uma área de TI. Exigir que os produtos finais dos serviços de programação finalizados sejam testados e revisados pela área de TI e outras partes envolvidas (tais como usuários, gerentes de projeto, etc.) antes do pagamento pelo trabalho e da aprovação do produto final.

- Contrato - O contrato deve estipular que o software, documentação e outros produtos estejam sujeitos a teste e revisão antes de sua aceitação. O teste a ser incluído nas especificações do contrato deve consistir em teste de sistema, de integração, de hardware e componentes, além do teste de procedimentos, carga e resistência, desempenho, regressão, aceitação por parte do usuário e, finalmente, teste piloto do sistema total para evitar qualquer falha inesperada do sistema.

- Definição de interfaces - Avaliar os controles para assegurar que todas as interfaces internas e externas sejam especificadas, projetadas e documentadas de forma apropriada.

- Materiais de Apoio e de Referência para Usuários - Verificar se são preparados manuais de apoio e de referência para usuários (preferivelmente em formato eletrônico) como parte de cada projeto de desenvolvimento ou modificação de sistemas.

### 4.2.2 – Instalar e aprovar sistemas

Definição de um dimensionamento de desempenho de aplicativo de software (otimização) como parte integral da metodologia de ciclo de vida de desenvolvimento de sistema da organização com o objetivo de prever os recursos exigidos para se operar software novo ou mudado de forma significativa.

Avaliar se para cada projeto de desenvolvimento, implementação ou modificação de sistemas de informação, foram implementados controles para

certificação se os elementos necessários do sistema antigo serão convertidos ao novo de acordo com um plano pré-definido.

Exigir que seja preparado um plano de conversão de dados, definindo os métodos de se coletar e verificar os dados a serem convertidos e identificando e resolvendo quaisquer erros encontrados durante a conversão.

Devem se executados testes incluindo a comparação de arquivos originais e convertidos, verificando a compatibilidade dos dados convertidos com o novo sistema, verificando arquivos principais após a conversão para assegurar a exatidão dos dados do arquivo principal e assegurando que as transações que afetam os arquivos principais atualizem os arquivos novos e antigos durante o período entre a conversão inicial e a implementação final.

Executar uma verificação detalhada do processamento inicial do novo sistema para confirmar o sucesso da implementação.

Verificar o procedimento de revisão de pós-implementação de sistema de informação operacional (por exemplo, capacidade, resultados, etc.) para avaliar se as necessidades dos usuários estão sendo satisfeitas pelo sistema.

### 4.2.3 – Gerenciar mudanças

Assegurar que todas as solicitações de alterações, manutenção de sistema e manutenção de fornecedor sejam padronizadas e estejam sujeitas aos procedimentos

formais de administração de mudança. As alterações devem ser categorizadas e priorizadas e devem existir procedimentos específicos para se lidar com assuntos urgentes. Os solicitantes de alterações devem ser mantidos informados sobre o status de sua solicitação.

O pessoal de manutenção deve possuir tarefas específicas e seu trabalho deve ser monitorado apropriadamente. Inclusive, controlando os direitos de acesso ao sistema para evitar riscos de acessos não autorizados a sistemas automatizados.

Deve ser assegurado conformidade com regulamentações sobre privacidade, propriedade intelectual, fluxo de dados e de criptografia aplicáveis às práticas de TI de uma organização, além de assegurar conformidade com padrões de segurança e de ergonomia no ambiente de trabalho dos usuários e equipe de TI.

## 4.3 – Entrega e Suporte

### 4.3.1 – Definir e gerenciar os níveis de serviço

Definir a estrutura promovendo acordos formais de níveis de serviços e seu conteúdo mínimo: disponibilidade, confiabilidade, desempenho, capacidade de crescimento, níveis de suporte oferecidos aos usuários, planejamento de continuidade, segurança, nível mínimo de satisfação com a funcionalidade do sistema, restrições (limites sobre o custo do trabalho), taxas de serviço e procedimentos de alterações. Os usuários e a área de TI devem ter um acordo por escrito que descreva o nível de serviço em termos qualitativos e quantitativos. O acordo define as responsabilidades de ambas as partes. A área de TI deve oferecer a qualidade e quantidade de serviço acordada e os usuários devem manter suas demandas sobre o serviço dentro dos limites acordados.

Deve ser nomeado um responsável por monitorar e reportar a obtenção dos critérios de desempenho de serviço especificados e todos os problemas encontrados durante o processamento. As estatísticas de monitoramento devem ser analisadas de forma oportuna. Ações corretivas apropriadas devem ser tomadas e as falhas devem ser investigadas.

### 4.3.2 – Gerenciar os serviços de terceiros

- Interfaces - Assegurar que todos os prestadores de serviços terceirizados sejam identificados apropriadamente e que sejam documentadas as interfaces técnicas e organizacionais com os fornecedores.

- Contratos - Definir procedimentos específicos para assegurar que para cada relacionamento com outros fornecedores de serviços seja definido e assinado um contrato formal antes do início do trabalho.

- Qualificação - Assegurar que, antes da seleção, os terceiros sejam apropriadamente qualificados através de uma avaliação de sua capacidade em prover os serviços necessários (due dilligence).

- Continuidade - Considerar o risco relacionado aos negócios de terceiros em termos de incertezas jurídicas e do conceito de going concern (funcionamento da empresa) e negociar contratos de caução quando apropriado.

- Relacionamentos de segurança - Assegurar que acordos de segurança (por exemplo, acordos de confidencialidade) sejam identificados e estejam acordados e satisfaçam padrões universais de negócios obedecendo a requisitos legais e regulamentares, inclusive obrigações.

- Monitoramento - Elaborar um processo para se monitorar a entrega de serviço de terceiros para assegurar que o acordo seja cumprido.

### 4.3.3 – Gerenciar o desempenho e a capacidade

Assegurar que as necessidades do negócio sejam identificadas com relação à disponibilidade e desempenho dos serviços de informação e convertidas em termos e requisitos de disponibilidade, implementando um processo para assegurar que o desempenho dos recursos de TI seja continuamente monitorado e as exceções sejam relatadas de forma oportuna e abrangente.

É necessário identificar ou resgatar controles para assegurar que as previsões de carga de trabalho sejam preparadas para identificar tendências e para fornecer informações necessárias para o plano de capacidade.

### 4.3.4 – Garantir a continuidade do serviço

Definição da estrutura de continuidade que defina os papéis, responsabilidades e a abordagem/metodologia baseada em riscos a ser adotada e as regras e estruturas para documentar o plano de continuidade, assim como os procedimentos de aprovação.

Assegurar que seja desenvolvido um plano por escrito contendo o seguinte:

• Diretrizes sobre como usar o plano de continuidade

• Procedimentos de emergência para assegurar a segurança de todos os membros de equipes participantes

• Procedimentos de resposta direcionados a recuperar o nível de negócios antes do incidente ou de ocorrências graves

• Procedimentos de recuperação direcionados a recuperar o nível de negócios antes do incidente ou de ocorrências graves

• Procedimentos para salvaguardar e reconstruir o local de trabalho

• Procedimentos de coordenação com autoridades públicas

• Procedimentos de comunicação com acionistas, funcionários principais clientes e fornecedores, quotistas e administração

• Informação crítica sobre as equipes de continuidade, a equipe envolvida, clientes, fornecedores, autoridades públicas e a mídia.

O plano de continuidade deve identificar os programas de aplicativos críticos, serviços de terceiros, sistemas operacionais, pessoal e materiais, arquivos de dados e horários necessários para recuperação depois que houver uma ocorrência grave. Identificar dados e operações críticas, de forma que sejam documentados, priorizados e aprovados pelos proprietários de processos empresariais, juntamente com a administração de TI.

Avaliar se, pela metodologia de continuidade para ocorrências graves, que todas as partes envolvidas receberam treinamento regular com relação aos procedimentos a serem seguidos no caso de um incidente ou ocorrência grave.

### 4.3.5 - Garantir a segurança dos sistemas

Avaliar os controles de restrição ao acesso lógico e uso de recursos de computação da área de TI, através da implementação de mecanismos de identificação,

autenticação e autorização adequados, integrando usuários e recursos a regras de acesso.

Criar ou resgatar procedimentos para manter ativos os mecanismos de acesso e autenticação (por exemplo, alterações de senha regulares). Tais mecanismos devem evitar que o pessoal não-autorizado, conexões dial-up e outras portas de entrada ao sistema (rede) acessem os recursos do computador e minimizem a necessidade de usuários autorizados usarem vários sign-ons.

Devem existir procedimentos para garantir ações tempestivas com relação a solicitação, definição, emissão, suspensão e cancelamento de contas de usuários, incluindo procedimento formal de aprovação destacando os dados ou proprietário de sistema garantindo os privilégios de acesso.

Assegurar que as atividades de segurança sejam registradas e que qualquer indicação de violação iminente de segurança seja relatada imediatamente a todos os interessados, interna ou externamente e que isso seja feito em tempo.

As políticas organizacionais devem contemplar as seguintes práticas de controle

- Partes-Confiáveis - verificar a autenticidade das partes que fornecem as instruções ou transações eletrônicas. Isso pode ser implementado através da troca protegida de senhas, tokens ou chaves de criptografia.

- Autorização de transação - oferecer autenticidade de transações e definir a validade de uma identidade de usuário declarada ao sistema. Isso requer o uso de técnicas de criptografia para indicar e verificar transações.

- Não rejeição - que as transações não possam ser negadas por qualquer uma das partes e que sejam implementados controles para garantir a não-rejeição de origem ou recebimento, comprovação de submissão e recebimento de transações. Isso pode ser implementado através de assinaturas digitais, registro de horário e partes confiáveis, com políticas apropriadas que levam em consideração requisitos regulamentares relevantes.

- Caminhos protegidos - que os dados de transações importantes só sejam trocados em caminhos protegidos. Informações importantes incluem gestão de informações de segurança, dados de transações importantes, senhas e chaves criptográficas. Para atingir isso, podem ser necessários canais protegidos através do uso de criptografia entre usuários, entre usuários e sistemas e entre sistemas.

- Deve ser avaliada a definição de uma estrutura de medidas de controle preventivas, de detecção e corretivas e resposta a ocorrências e métodos de reportagem com relação a software destrutivo, tal como vírus de computador ou Cavalos de Tróia. Assegurar que sejam definidos procedimentos em uma organização para proteger sistemas de informação e tecnologia de vírus de computador. Os procedimentos devem incorporar a proteção a vírus, sua detecção, resposta a ocorrências e métodos de reportagem.

- Os firewalls devem ser adequados para proteção contra negação de serviços e qualquer acesso não-autorizado aos recursos internos. Devem controlar quaisquer aplicativos e fluxos de gestão de infra-estrutura em ambas as direções; e devem proteger contra ataques de negação de serviço.

### 4.3.6 – Gerenciamento dos dados

Verificar os controles de validação dos dados da transação entrados para processamento (gerados por pessoas, por sistema ou interface) a vários controles para verificação de precisão, totalidade e validade. Os procedimentos devem ser apropriados para assegurar que seja executada entrada de dados somente por pessoal autorizado e garantido a separação de tarefas e verificação rotineira do trabalho. Deve ser dispensada especial atenção a autenticação e integridade de informações originadas fora da organização, recebidas por telefone, correio de voz, documento em papel, fax ou e-mail, antes que seja tomada ação potencialmente crítica.

Assegurar que seja oferecida proteção de informações importantes durante a transmissão e transporte contra acesso, modificação e uso não autorizados. Definir os períodos de retenção e condições de armazenagem para documentos, dados, programas, relatórios e mensagens (de entrada e saída), assim como os dados (chaves, certificados) usados para sua criptografia e autenticação.

Avaliar a estratégia de back-up e restauração a fim de assegurar que a área de TI inclua uma revisão de requisitos de negócios, assim como o desenvolvimento, implementação, teste e documentação do plano de recuperação. Os back-ups devem

ser armazenados de forma segura e vistoriados os locais de armazenagem periodicamente com relação à segurança de acesso físico e à segurança de arquivos de dados e outros itens.

### 4.3.7 – Gerenciamento das instalações

Avaliar as medidas de controle de acesso e de segurança física apropriadas para as instalações de TI, incluindo uso de dispositivos padrões fora do local de trabalho de acordo com a política geral de segurança. Tratar a segurança física e controles de acesso não somente da área contendo o hardware, mas também dos locais de cabeamento usados para conectar elementos do sistema, serviços de apoio (tais como eletricidade), mídia de back-up e quaisquer outros elementos necessários para a operação do sistema. Restringir o acesso a indivíduos que foram autorizados a obter tal acesso.

Garantir que existam e que sejam mantidas medidas suficientes para a proteção contra fatores ambientais (por exemplo, incêndio, pó, eletricidade, calor excessivo e umidade). Instalar equipamentos e dispositivos especializados para monitorar e controlar o ambiente.

## 4.4 – Monitoramento

### 4.4.1 – Monitorar os processos

Mensurar os serviços a serem prestados pela área de TI (indicadores chave de desempenho e/ou fatores críticos de sucesso) e comparar com as metas. Executar avaliações da área de TI continuamente.

Os relatórios devem ser fornecidos a alta administração para que esta revise o progresso da organização com relação às metas identificadas. Incluir nos relatórios de status até que ponto os objetivos e resultados planejados foram atingidos, até onde as metas de desempenho foram satisfeitas e os riscos mitigados. Indicar e controlar a ação por parte da administração, mediante revisão.

## 5 – Avaliação da Gestão do Risco de Mercado

Em Duarte (2005) o risco de mercado é associado a vários riscos, como taxa de juros, risco de taxas de câmbio, risco de ações, risco de *commodities*, risco de liquidez, risco de derivativos, risco de *hedge* e risco de concentração.

O processo de avaliação de qualquer instituição financeira, especialmente àquelas focadas para as operações de Tesouraria, passa, fundamentalmente, pela avaliação de como esses riscos são geridos. Neste contexto, algumas práticas são amplamente utilizadas e serão utilizadas como benchmarking no processo de avaliação dos controles internos, cabendo um papel especial a definição de limites diversos.

### 5.1 – Limites de Riscos de Mercado

O Risco de limites em uma instituição financeira é um risco extremamente difícil de gerenciar de forma eficiente e que geralmente requer um elevado investimento, especialmente em sistemas. Adicionalmente, é um risco altamente exposto ao fator humano e, por isso, a cultura de controle da instituição é um fator crítico no processo.

Talvez por isso pode ser considerado um dos principais riscos de uma instituição financeira com foco em operações de Tesouraria

A seguir exploraremos os principais fatores críticos a serem avaliados dentro da estrutura do sistema de controles internos

- Organização

Inicialmente, o risco de limites deve ser avaliado na própria definição da estrutura organizacional da instituição. Neste contexto, o Comitê da Basiléia (1998) menciona como princípio básico de controle pela administração e cultura de controle, a existência de um conselho ou comitê responsável pela aprovação das estratégias e políticas bem como a estrutura organizacional operante.

A Tesouraria deve ser subordinada à alta diretoria ou um comitê financeiro que é efetivamente responsável pela decisão quanto aos limites da tesouraria e a política de investimentos para a área de tesouraria.

Adicionalmente, estas políticas devem ser estabelecidas de maneira clara e objetiva de forma a não criar espaço para negligências. É importante que a alta administração acesse constantemente suas definições, adaptando-as às mudanças de condições de mercado, de maneira suficientemente flexível.

Adicionalmente, é importante avaliar o nível de envolvimento da alta diretoria nas decisões estratégicas. O Comitê da Basiléia (1994) ressalta que o Conselho e a Alta Gerência devem ser ativos no processo de gerenciamento de risco e devem acreditar que a gerência de risco é um essencial do negócio, onde investimentos relevantes devem ser feitos. Neste contexto, os relatórios diários devem ser

constantemente revistos por um nível de gerência que possui a senioridade e a autoridade suficiente para demandar a redução das posições tanto individuais como da instituição como um todo.

- Independência

As instituições financeiras devem possuir uma unidade de gerenciamento de risco independente das operações com o objetivo de garantir maior segurança e transparência nas informações.

Esta unidade de gerenciamento de risco costuma estar ligada diretamente à Presidência, sendo sua atribuição o cálculo do risco de mercado e a geração dos relatórios diários com os resultados. Por outro lado, a unidade de gerenciamento de risco deve ser integrada ao gerenciamento das operações e conhecer as estratégias operacionais.

Com base nas aprovações dos riscos diversos (mercado, liquidez e outros) pela Alta Administração, o departamento responsável por gerenciar os riscos (middle-office) calcula as exposições aos respectivos riscos e os excessos são reportados aos operadores e a alta administração.

- Conflito de Interesse

Os funcionários e especialmente os *traders* devem agir de acordo com interesse somente do empregador na realização das tarefas. O conflito de interesse

surge quando o funcionário tem algum grau de parentesco, amizade ou interesse financeiro na transação, a qual pode conflitar com seus interesses e, consequentemente, trazer prejuízo para a instituição financeira.

Neste contexto, todo o processo de definição, monitoramento e aprovação dos limites deve estar livre do risco do conflito de interesse.

- Aplicabilidade

O modelo utilizado para o gerenciamento do risco de mercado deve ser integrado ao gerenciamento diário do risco de mercado, ou seja, os resultados devem ser partes integrantes do processo de planejamento, monitoramento e controle do perfil de risco de mercado da instituição financeira. Neste contexto, os limites devem estar relacionados com os modelos de risco de forma consistente ao longo do tempo, sendo de conhecimento tanto dos traders, como da Alta Administração.

A seguir são apresentados alguns limites que podem ser estabelecidos e aprovados pela Alta Administração no gerenciamento dos riscos da tesouraria.

- Value-at-Risk

O VaR é uma das principais medidas da instituição de risco da carteira e a definição de limites para essa medida é fundamental para o gerenciamento de risco e a administração da decisão estratégica. Em Duarte (2005) é ressaltado que os limites baseados no *value-at-risk* estejam sempre presentes na gestão de riscos de mercado e

devem cobrir todos os fatores de mercado existentes (relacionados a ações, *commodities*, taxas de câmbio e taxas de juros).

- Bloqueio de perdas (*Stop-Loss*)

Uma regra de stop-loss consiste em impor um limite para as perdas acumuladas por uma determinada posição, reduzindo o risco que os operadores apresentem resistência ao abandonar as estratégias após uma perda relevante, esperando que o mercado se altere. Contudo, caso o mercado não se altere, existe a possibilidade das perdas tornarem-se ainda maiores.

Uma alternativa é impor um limite máximo para perdas acumuladas num determinado horizonte de tempo e rompido este limite, determinar a liquidação da posição.

- Limites de Liquidez

Definição de limites para operações com produtos pouco líquidos que dificilmente podem ser liquidados no mesmo dia. Exploraremos o risco de liquidez de forma mais abrangente no capítulo 6.

- Limites individuais.

São definidos para controlar as operações de forma individualizada. É importante que os limites estejam estabelecidos de acordo com o nível de senioridade dos operadores.

- Limites de estresse

São os limites definidos a partir da simulação da carteira com base em cenários hipotéticos, sendo importante para complementar o limite do VaR.

### 5.1.5 - Eficiência

Outro aspecto relevante no monitoramento dos limites refere-se à eficiência no processo. Neste contexto, um aspecto fundamental refere-se ao monitoramento em tempo real dos limites estabelecidos pela Alta Administração, incluindo a existência de mecanismos de alertas que reduzam o risco de realização de operações não autorizadas, seja por erro intencional ou não. Esse mecanismo atuaria como um controle preventivo na verificação do cumprimento dos limites.

Jorion (1997) ressalta que a implantação do monitoramento do risco em "tempo real" envolve a automatização do fluxo de dados de cada transação, dirigindo-os para a unidade de gerenciamento de risco, bem como, de liquidação e registro, determinando um investimento significativo em tecnologia de informação.

O monitoramento dos limites em tempo real constitui um obstáculo ainda a ser superado por diversas instituições financeiras, à medida que as unidades de gerenciamento de risco ainda não são capazes de monitorar as exposições de forma preventiva ao longo do dia e em tempo real.

Se os limites precisam ser ultrapassados, devem ser devidamente autorizados, por escrito, antes da negociação.

Ao avaliar a eficiência dos controles sobre os limites de uma instituição financeira, identifiquei que as não conformidades eram identificadas pelo pessoal do middle-office somente no dia seguinte e por volta das 11:00 hs da manhã. Após identificação da falha e comunicação à Alta Administração, os horários dos funcionários foram alterados e realizados altos investimentos tecnológicos, que inclui a redução da utilização de planilhas eletrônicas, que permitiram à instituição o cálculo dos limites à cada 5 minutos. Desta forma, o controle sobre os limites passou a apresentar um caráter mais preventivo e não detectivo.

### 5.1.6 – Formalização

Todo o processo de escolha dos tipos de limites, definição de valores, monitoramento e violações devem estar devidamente formalizados e armazenados para avaliação das justificativas pelos auditores e órgãos reguladores.

## 6- Avaliação da Gestão do Risco de Liquidez

O Risco de Liquidez está associado à capacidade de comprar/vender um ativo sem afetar substancialmente o preço. As instituições financeiras devem ser capazes de avaliar as alterações dos preços nos cenários de estresse e o subseqüente impacto no valor da carteira, ou seja, é necessário avaliar as alterações na liquidez dos mercados.

Segundo Carvalho (2003) dentre os vários tipos de riscos a que um banco está exposto em sua rotina, o de liquidez é um dos que requerem maior atenção, já que pode levar qualquer instituição financeira ao colapso rapidamente.

É possível que determinadas transações sejam difíceis ou quase impossíveis de serem executadas com base em um razoável spread de compra e venda durante o período de estresse do mercado. Neste contexto, por exemplo, ao comprar um contrato futuro para hedgear um ativo ou instrumento financeiro ilíquido, deve ser considerado a disponibilidade de recursos para manter o contrato futuro em carteira, ou seja, os ganhos e perdas dos contratos são reconhecidos imediatamente através dos ajustes diários, ao passo que para o outro ativo isso pode não ser verdade, sendo que o reconhecimento é feito somente no vencimento da operação.

Consequentemente, mesmo uma posição bem hedgeada pode levar a descasamento de tempo no que tange ao recebimento e pagamento dos recursos. Desta forma, a avaliação do teste de estresse passa, necessariamente, pelo risco de liquidez.

De acordo com a Resolução 2804/00 do Banco Central do Brasil, as políticas e os procedimentos mínimos a serem adotados no gerenciamento do risco de liquidez são:

1) Manter de forma adequadamente documentada os critérios e a estrutura estabelecidos para o controle do risco de liquidez;

2) Elaborar análises econômico-financeiras que permitam avaliar o impacto dos diferentes cenários na condição de liquidez de seus fluxos de caixa, levando em consideração, inclusive, fatores internos e externos à instituição;

3) Elaborar relatórios que permitam o monitoramento dos riscos de liquidez assumidos;

4) Realizar avaliações voltadas à identificação de mecanismos e instrumentos que permitam a obtenção dos recursos necessários para reversão de posições que coloquem em risco a situação econômico-financeira da instituição, englobando as alternativas de liquidez disponíveis nos mercados financeiros e de capitais;

5) Realizar periodicamente testes de avaliação dos sistemas de controle implantados, incluindo testes de estresse, testes de aderência e quaisquer outros que permitam a identificação de problemas que, de alguma forma, possam comprometer o equilíbrio econômico-financeiro da instituição;

6) Promover a imediata disseminação das informações e análises empreendidas sobre risco de liquidez aos diversos setores diretivos e gerenciais da instituição, bem como as conclusões e providências adotadas;

7) Estabelecer plano de contingência contendo estratégias de administração de situações de crise de liquidez.

A seguir apresentaremos ferramentas obrigatórias na gestão do risco de liquidez, ressaltando os principais aspectos a serem observados na avaliação desses controles.

## 6.1 – Fluxo de Caixa

A instituição que gerencia com eficiência o risco de liquidez entende o processo e monitora constantemente este risco. Neste contexto, podem ser utilizadas diversas técnicas para mensurar o risco de liquidez. No entanto, o controle básico sobre a gestão do risco de liquidez consiste na identificação das deficiências futuras no fluxo de caixa, ou das necessidades líquidas de captação. Devem, então, ser estabelecidos diversos cenários que possibilitem avaliar o comportamento futuro de seus ativos, passivos e itens registrados "fora do balanço" ao longo de uma série de períodos de tempo. A análise de fluxo de caixa deve permitir, entre outros:

- Disponibilização de fluxos de caixa distintos por produto ou mercado;
- Disponibilização fluxos de caixa distintos para as operações com ou sem garantia;
- Permitir a remoção de qualquer produto do fluxo de caixa e a inclusão do mesmo no saldo inicial, com algum deságio, considerando prazos de liquidação específicos;
- Permitir uso de alarmes quando limites pré-estabelecidos de saldos forem superados;
- Permitir a avaliação dos cenários em dias, semanas, meses e anos;
- Permitir a realização de simulações sem alterar os fluxos originais;
- Permitir a entrada de dados para hipóteses de TR, IGP´S, TJLP, US$ e CDI visando a simulação dos fluxos de caixa;

- Permitir a inclusão de valores nos fluxos de caixa simulados;
- Permitir a eliminação de quaisquer fluxos de caixa eleitos nos fluxos de caixa simulados;
- Permitir a alteração dos valores de resgates de passivos nos fluxos de caixa simulados.

Os relatórios de estresse no fluxo de caixa devem considerar os referidos fatos e são emitidos para os responsáveis pela gestão do risco de liquidez.

**6.2- Plano de contingência de liquidez**

Os planos de contingência podem ser desenvolvidos para certos cenários. Apesar da ineficácia dos planos de contingência na recuperação do valor dos ativos, eventuais descasamentos de recursos ocasionados pela futura demanda de caixa, podem ser gerenciados com recursos planejados pelos planos de contingência.

A avaliação do plano de contingência da instituição aborda, pelo menos, a existência das seguintes características:

- Descrição das obrigações detalhadas do pessoal chave numa situação de crise;
- Definição e quantificação periódica das fontes de recursos vulneráveis e não vulneráveis, bem como dos ativos líquidos;
- Definição da volatilidade de mercado necessária para o equivalente encurtamento dos ativos e redução de operações de crédito;

Ainda na avaliação do Plano de Contingência, o Banco Central do Brasil no Manual de Supervisão Bancária recomenda a quantificação de:

- Fontes de recursos que provavelmente continuarão com a instituição em qualquer circunstância e se tais fundos podem ser incrementados;
- Fontes de recursos que deverão se retrair gradualmente caso surjam problemas;
- Preço dos depósitos necessários para controlar a velocidade dos saques;
- Tipos de passivos com vencimentos não-contratuais que possam ser sacados de imediato;
- Montante dos passivos cujo saque antecipado é provável;
- Linhas de reserva que a instituição pode sacar e em que circunstâncias

## 6.3- Modelagem do Risco de Liquidez

É importante avaliar como os gestores de mercado incorporam o risco de liquidez nas ferramentas de gestão de risco, cuja importância aumentou com a experiência vivida nas últimas crises ocorridas no mercado financeiro internacional nos anos 90 (Crise da Rússia e Ásia), em que a liquidez, ou a falta da mesma, desempenhou importante papel na intensidade e duração das mesmas.

Vicente (2003) menciona que conforme O'Hara (1995), muito embora mercados líquidos sejam facilmente reconhecíveis à primeira vista, os fatores que determinam a liquidez desses mercados nem sempre são óbvios, podendo o mesmo ser dito com relação ao risco de liquidez, ou seja, o conceito de liquidez varia de acordo com a ênfase dada aos aspectos de mercados (fatores exógenos) e às características da posição detida em determinado ativo (fatores endógenos).

Ainda segundo o autor, os modelos de risco de liquidez são divididos nessas duas grandes classes. Enquanto os modelos exógenos consideram insignificante o impacto causado pela atividade de um único participante, modelos de liquidez de origem endógena reconhecem que, em mercados pouco líquidos, a atividade de um único participante pode exercer considerável pressão sobre os preços dos ativos. Em virtude de sua complexidade e dos dados necessários à sua estimação, essa última classe ainda apresenta poucas alternativas que possam ser implementadas de forma prática e consistente.

Conforme ressaltado por Bangia (1998), é importante modelar o risco de liquidez à medida que variações no risco de liquidez exógeno são geralmente grandes e relevantes, atingindo todos os participantes do mercado de forma indiscriminada e, ao contrário do que ocorre com a estimação do risco de liquidez endógeno, os dados necessários para sua estimação são de fácil obtenção, tornando possível sua implementação prática.

Por outro lado, em função da complexidade, ainda hoje, Vicente (2003) ressalta que existem poucos modelos quantitativos formais que se proponham a incorporar o risco de liquidez endógena na estrutura de estimação do risco de mercado.

Em nossa avaliação da gestão do risco de liquidez, mais do que simplesmente avaliar como o risco de liquidez é mensurado e, consequentemente, incorporado aos modelos de risco de mercado, é importante avaliar como os gestores lidam com as

restrições impostas pela dificuldade de assumir certas premissas. Adicionalmente, cabe avaliar, mais uma vez, a transparência na divulgação dessas limitações.

## 7 – Avaliação do Risco de Modelagem

Em Duarte (2005), o risco de modelagem está associado a perdas potenciais devido ao fato de os modelos matemáticos não serem adequadamente desenvolvidos e utilizados e, seus resultados, entendidos.

Em Duarte (1997), é ressaltado que todos os modelos matemáticos utilizados nas instituições financeiras são partes do que é comumente chamado de "Procedimento de Decisão Matemática" (PDM). Ainda segundo o autor, entender esses procedimentos simplifica a explicação dos impactos do risco de modelagem no processo de tomada de decisão para as instituições financeiras.

Neste contexto, o autor ressalta que o PDM apresentou um significativo progresso no mercado financeiro e sua importância vem aumentando ao longo do tempo em função de quatro razões:

- Aumento da quantidade de dados a serem processados e da inter-relação entre os importantes fatores a serem entendidos, ou seja, os PDM são importantes porque transformam dados em informações;
- A redução dos custos tecnológicos, acompanhado de uma melhora dos mesmos, ajudou o PDM nas instituições financeiras;
- As tomadas de decisões estão ficando mais automáticas e independentes, assim como os produtos financeiros;
- Aumento da necessidade de obtenção de respostas rápidas para decisões de problemas em tempo real.

Segundo Longo (2005), o gerenciamento do risco de mercado teve o grande benefício do surgimento de um modelo que se tornou padrão em função das suas qualidades. Segundo o autor, ao tornar pública em 1994, a metodologia RiskMetrics$^{TM}$, O J.P. Morgan deu uma contribuição decisiva para o gerenciamento do risco de mercado. O cálculo do Value-at-Risk (VaR) foi adotado como o melhor modelo para quantificar o risco de mercado e tem sido utilizado, inclusive para efeitos regulatórios, tais como o cálculo do capital a ser alocado em função dos riscos incorridos.

Duarte (2005) menciona que as seguintes questões devem ser analisadas quando da avaliação da eficiência de um modelo matemático:

- Todos os parâmetros e variáveis foram incluídos no modelo? Existe algum outro parâmetro ou variável que alteraria o resultado de forma significativa?
- Todas as premissas sobre a dinâmica das variáveis foram verificadas? Foram realizados testes estatísticos para verificar se as hipóteses feitas sobre as variáveis podem ser rejeitadas com base nos resultados passados?
- Os resultados obtidos estão em conformidade com os observados no mercado? O modelo prevê de forma precisa os resultados do problema modelado?

A seguir apresentamos as principais fontes de exposição ao risco de modelagem:

## 7.1- Value-at-Risk

Em Jorion (1997), o VaR é definido como uma medida da pior perda esperada dentro de certo intervalo de tempo, em condições normais de mercado e a um certo nível de confiança. É uma medida monetária, sendo bastante fácil de ser compreendida. Assim, se um banco informar que o VaR diário de sua carteira é de R$1 milhão, com um nível de confiança de 99%, a informação subjacente é que há apenas uma chance em cem de que ao longo de um dia o prejuízo supere R$1 milhão, considerando condições de mercado.

### 7.1.1- Escolha das premissas

Uma das principais dificuldades encontradas no VaR diz respeito a escolha das suas premissas. Neste contexto, é fundamental o envolvimento da Alta Administração na escolha e conseqüente aprovação das referidas premissas. Para isso, é importante que antes da efetiva aprovação, seja devidamente avaliadas as alternativas existentes e os respectivos custos e benefícios, de forma que as premissas escolhidas sejam as mais aplicáveis aos interesses da instituição financeira e, consequentemente, dos acionistas.

É importante ressaltar que as escolhas podem não necessariamente ser melhores ou piores do ponto de vista matemático, mas sim premissas que melhor atendam o objetivo estratégico do cálculo do VaR. Neste contexto, vale ressaltar que todos os modelos matemáticos estão sujeitos a erros, sendo assim, os mesmos devem ser vistos como uma aproximação do resultado observado no mundo real.

Por exemplo, o VAR pode ser condicional ou incondicional. Para estimar o VaR condicional, é necessário estimar total ou parcialmente a função de distribuição condicional dos retornos, por exemplo, normal. Em situações de cálculo de VaR a 5% ou mais, a utilização da distribuição normal condicional mostra-se adequada. Entretanto, para os modelos com VaR de probabilidades mais baixas, é maior a probabilidade de erro pelo uso da aproximação normal, pois subestima a ocorrência de eventos extremos, ou seja, a aproximação pela distribuição normal falha na cauda da distribuição. Apesar das limitações, sem dúvida o cálculo do VaR se torna bem mais fácil quando assumimos a hipótese de que a distribuição dos retornos dos ativos de mercado segue uma distribuição normal, o que resulta em menores esforços operacionais, tais como, computacionais e de pessoal, o que pode ser interessante para a Alta Administração do ponto de vista de redução de investimentos, vis-à-vis a relação custo / benefício.

Outra importante premissa é o horizonte de tempo. Neste contexto, a escolha de horizontes de tempo superiores a 1 dia pode comprometer a eficácia do cálculo do VaR estimado com base na metodologia de Variância-Covariância. Isto porque esta metodologia é baseada em aproximação linear que não funciona nos instrumentos com cláusulas de opção.

As metodologias de simulação histórica ou de Monte Carlo funcionam com maior nível de confiança, independente da existência de opcionalidade, porque a metodologia recalcula o valor da carteira supondo alterações nos fatores de risco e,

consequentemente, calculando “corretamente” a distribuição dos valores da carteira. Contudo, ambas são limitadas em determinados aspectos.

A distribuição dos valores da carteira pela simulação de Monte-Carlo depende da premissa utilizada para a distribuição dos fatores de risco e das estimativas dos seus parâmetros, onde ambos podem ser errados e, consequentemente, gerar erros no cálculo do VaR. De forma análoga, a distribuição dos valores da carteira estimados com base no modelo de simulação histórica pode ser errada caso os N dias prévios utilizados para realizar a simulação não sejam relevantes ou repliquem a realidade futura.

Em Duarte. (1997) é demonstrado a importância da escolha do modelo utilizado para o cálculo do VaR. Foi assumida a seguinte carteira hipotética no dia 10 de setembro de 1996:

- Posição comprada de 13 milhões de ações da Telebrás PN ao preço de 18,50 por mil ações;
- Posição comprada de 70 mil ações de Vale PN ao preço de R$21,00 por ação;
- Posição vendida de 25 milhões de opções de compra americana de Telebrás PN com vencimento em 21/10/96 ao preço de exercício de R$80,00 por mil ações;
- Posição vendida de 112 mil opções de compra americana de Vale PN com vencimento em 21/10/96 ao preço de exercício de R$20,83 por ação;

Ao estimar o VaR de 1 dia, ao nível de confiança de 5%, foram obtidos diversos resultados, alguns apresentando diferenças significativas, conforme o modelo

utilizado. A tabela a seguir foi apresentada pelo autor para demonstrar os diferentes resultados:

Tabela 9: Cálculo do VaR pelas diferentes metodologias

| **Metodologia de cálculo** | |
|---|---|
| Método analítico utilizando o Delta – equivalente | R$559,32 |
| Método analítico utilizando o mapeamento dos fatores de risco | R$27.247,80 |
| Método analítico utilizando a aproximação de Cornish-Fisher | R$23.801,19 |
| Simulação Histórica | R$13.904,95 |
| Simulação de Monte-Carlo | R$11.404,72 |

Entre as premissas a serem definidas, recomendamos as seguintes:

Sistema: Paramétrico, Não-Paramétrico

Metodologia: RiskMetrics, Monte-Carlo, Simulação Histórica, Variância-Covariância, combinação.

Horizonte de tempo: 1 dia, 10 dias

Nível de confiança: 99%, 97,5%, 95%

Volatilidade: Desvio-padrão histórico, Alisamento exponencial, Modelo GARCH

A escolha das premissas também passa pelo nível de conhecimento da Alta Administração sobre o cálculo do VaR. Neste contexto, a metodologia de simulação histórica é simples de ser entendida. Por outro lado, para um público com pouco conhecimento técnico, o entendimento dos principais passos da metodologia de

variância-covariância pode ser um obstáculo de difícil superação e isto se torna mais crítico para a metodologia de Monte Carlo.

O grande desafio dos responsáveis por avaliar a eficiência dos controles internos é conhecer as vantagens e as limitações do modelo utilizado pela respectiva instituição financeira e verificar se os responsáveis conhecem os riscos envolvidos, especialmente a Alta Administração, atentando para a formalização dos fatos.

### 7.1.2- Mapeamento dos fatores de risco

Ao calcular o VaR, ou qualquer outra medida quantitativa de risco de mercado, é necessário identificar as taxas básicas e preços de mercado que afetam o valor da carteira quando da utilização do modelo paramétrico. Essas taxas básicas e preços de mercado que afetam o valor da carteira são chamados de “fatores de risco”.

No modelo de VaR paramétrico, os ativos, passivos e derivativos presentes na carteira são normalmente decompostos nos chamados fatores de risco, ao invés do tratamento de cada produto separadamente.

Person e Linsmeier (1994) ressaltam que é importante identificar um número limitado de fatores de risco, caso contrário a complexidade de mensurar o risco quantitativo da carteira aumenta de forma explosiva.

Um aspecto fundamental é entender que a correta avaliação do risco de mercado depende da consolidação das suas posições nos diversos instrumentos financeiras do seu portfolio.

A avaliação do modelo passa pela análise da decomposição dos fatores de risco que afetam os referidos ativos. O objetivo é analisar cada produto como um conjunto de fatores de risco que podem ser desmembrados; assim, ao selecionar os produtos que serão mantidos uma posição, uma instituição está, na realidade, selecionando os fatores de risco em que deseja ter algum tipo de exposição. O processo de selecionar os fatores de riscos que dependem de cada instrumento é chamado de “mapeamento de risco”. Na prática, o processo consiste em transformar as posições da carteira atual em um conjunto de posições padrões mais simples, sendo questão crucial na avaliação do risco de modelagem a verificação do mapeamento dos fatores de risco por instrumento financeiro.

Neto e Urban (2003) apresentam a tabela abaixo relacionando importantes ativos negociados por instituições financeiras brasileiras a seus fatores de risco.

Tabela 10: Mapeamento de fatores de riscos

| | Estrutura a termo | | | Mercados a vista | | | |
|---|---|---|---|---|---|---|---|
| | Pré | Cupom | Dolar a vista | Bolsa local | Bolsa externa | Bradies | Volatilidade |
| Futuros de dólar | * | * | * | | | | |
| Opções de dólar | * | * | * | | | | * |
| Papéis cambiais | | * | * | | | | |
| Futuros de DI, CDBs, swaps, pré, papéis pré | * | | | | | | |
| Ações locais | | | | * | | | |
| Futuros termos de ações | * | | | * | | | |
| Opções de ações | * | | | * | | | * |
| Ações externas | | | | | * | | |
| Bradies | | | | | | * | |

Ao avaliar o risco de modelagem em uma instituição financeira, identifiquei a ausência do fator de risco geralmente conhecido como “ágio/deságio sobre LFT”. Trata-se de um fator de risco que na época da crise da “marcação a mercado” (2002) passou a ser extremamente importante. Desta forma, foi incluído no referido relatório a sugestão de inclusão do referido fator de risco no modelo de cálculo do Value-at-Risk.

Além da própria identificação devida dos fatores de risco, é importante atentar para o tratamento utilizado no modelo no que se refere aos seguintes fatos:

- Mapeamento da estrutura a termo da taxa de juros.

Os instrumentos financeiros, geralmente, possuem diversos fluxos de caixa, cada um ocorrendo em determinado período de tempo. Consequentemente, para evitar

a geração de diversas correlações e volatilidades, é feito a simplificação da estrutura a termo.

Neste contexto, é necessário atentar para a quantidade de vértices e a escolha dos mesmos. Ressaltamos que o risco é maior nas estruturas a termo de juros internacionais, tais como, taxas de juros do tesouro americano, de Euro e YEN, onde é maior o risco da não utilização de vértices ou simplificações extremas dos mesmos.

- Não linearidade

Longo (2005) define não linearidade como aquela que apresenta uma mudança no seu valor numa proporção constante em relação a uma mudança no preço ou taxa de mercado, dada qualquer variação de preço.

Quando um instrumento tem um comportamento não linear, fator este encontrado mais comumente nos instrumentos com cláusula de opcionalidade, é indevido realizar a modelagem de forma paramétrica (Modelo de Variância-Covariância), ou seja, multiplicando as mudanças estimadas nos preços pela sensitividade da posição às mudanças, sendo mais aplicável a utilização de metodologias de simulação, tal como, Monte Carlo. Neste caso, deve ser atentado, inclusive, para o número mínimo de simulações, que geralmente é feito em torno de 5.000 cenários.

Neste contexto, a mitigação do risco de modelagem passa pela avaliação do comportamento dos instrumentos e, principalmente, a verificação de cláusulas de opcionalidade nos contratos.

- Combinações de instrumentos financeiros expostos ao mesmo fator de risco

Como a exposição a determinado fator de risco pode ocorrer, ao mesmo tempo, em diversos instrumentos financeiros, tais como, opção e ativo à vista, é necessário calcular o VaR da carteira de forma combinada para os dois instrumentos. A justificativa reside no simples motivo de que o mesmo ativo não pode assumir valores distintos em determinado instante do tempo, ou seja, não é correto estimar que, no mesmo horizonte temporal, o VaR das opções é calculado quando o ativo objeto assume o valor X e, ao mesmo tempo estimar que o VaR do ativo à vista ocorre quando o ativo objeto assume o valor Y, onde X é diferente de Y.

O risco é maior para o cálculo de modelos de VaR que combinam metodologias paramétricas e não-paramétricas, este último utilizada especialmente para os instrumentos com cláusula de opcionalidade para a resolução de problemas de não linearidade

### 7.1.3- Cálculo da volatilidade

O cálculo da volatilidade é uma das principais variáveis do VaR, sendo um dos principais pontos da maior parte dos artigos e estudos cujo pano de fundo é o cálculo do VaR.

O conceito de volatilidade está associado à previsibilidade em relação ao retorno dos ativos. Desde o início da chamada finanças modernas, em meados dos anos cinqüenta com a Teoria Moderna de Carteira de Markowitz, o cálculo da volatilidade vem sendo profundamente analisado.

Inicialmente a volatilidade estava associada ao conceito de desvio-padrão dos retornos, entretanto, os modelos evoluíram nos últimos anos impulsionados por, entre outros fatores, os avanços tecnológicos que possibilitaram a realização de cálculos matemáticos em tempos recordes.

Entre estes modelos, os mais comuns são os modelos da família GARCH e EWMA (média móvel exponencialmente ponderada), sendo o último mais comumente adotado nas instituições por apresentar a vantagem de ser de baixa complexidade e reagir rapidamente a um choque de mercado, captando a maior ou menor volatilidade mais prontamente.

É importante a avaliação do modelo utilizado para cálculo da volatilidade, atentando para a correta utilização do mesmo.

### 7.1.4- Cálculo da correlação

O coeficiente de correlação é outra premissa extremamente sensível no cálculo do VaR.

O conceito de correlação está associado à previsibilidade do retorno de um ativo, dado o retorno de outro ativo.

A Teoria Moderna de Carteira de Markowitz baseia-se no efeito provocado pela correlação para sugerir modelos de gerenciamento de riscos.

Independente da metodologia de cálculo da correlação que, assim como o desvio-padrão, podem ser calculadas de diversas formas, tais como, média móvel, ponderada ou aritmética e, por conseguinte, validada pelos auditores, é importante ressaltar o procedimento estabelecido para modelagem da correlação em situações excepcionais.

É comum observar redução na eficiência da diversificação em períodos de maior volatilidade, quando ocorre o aumento da correlação entre as ações. Desta forma, é importante avaliar a gestão desse risco na modelagem do VaR, atentando para o procedimento utilizado para o cálculo da correlação nos momentos de turbulência de mercado.

## 7.2- Teste de estresse

O VaR é deficiente em períodos de modificação do padrão de comportamento dos dados, afinal, um modelo probabilístico baseado em estatísticas históricas não será capaz de capturar as dimensões possíveis de movimentos bruscos nunca antes observados.

Para compensar essa deficiência e tornar o gerenciamento de risco de mercado abrangente e completo deve ser utilizado o Teste de estresse, que consiste em recalcular o valor da carteira para alguns cenários, ou combinação deles, representativos de situações de crises ou choques nos mercados que afetam a carteira.

O chamado teste de estresse ou análise de cenários, determina o impacto sobre o valor de mercado da carteira derivado de mudanças hipotéticas nos preços e taxas de mercado.

Diferente dos modelos de VaR, que em geral trabalham com volatilidades e correlações históricas, é comum que os cenários definidos nos modelos de estresse representem situações extremas e muitas vezes subjetivas.

A combinação específica de preços que determina cada cenário é uma decisão árdua. Dado que o objetivo do estresse é tentar prever uma realidade distante do dia-a-dia, mas, por outro lado, próxima do que poderia ocorrer em uma forte mudança das condições de mercado, é difícil, mesmo para os gestores de risco de mercado mais experientes, mapear esses cenários.

Contudo, apesar das dificuldades inerentes ao processo, é preciso realizar uma avaliação, pelo menos mínima, do risco de modelagem inerente no processo.

A seguir apresentamos as principais avaliações necessárias quando da escolha dos cenários:

### 7.2.1- Subjetividade

Neto e Urban (2003) mencionam que a escolha das tempestades, ou seja, dos cenários de estresse, envolvem um alto grau de subjetividade, a qual é mais intensa no momento em que as variações de preços específicas têm de ser combinadas entre si. Numa carteira com múltiplos ativos, as combinações específicas entre os preços são tão ou mais importantes que as magnitudes de variação de cada um, quando considerados individualmente. A conseqüência disso é que os resultados do modelo podem se tornar completamente sem sentido. Neste contexto, é importante para o auditor ou compliance officer avaliar a razoabilidade mínima dos cenários simulados e a experiência de crises passadas podem ser um bom parâmetro para as discussões.

Caso o gestor do risco de mercado utilize cenários bastante diferentes dos observados nas crises anteriores, é importante que a premissa seja bem fundamentada e que a mesma não seja simplesmente cenários escolhidos aleatoriamente.

### 7.2.2- Opcionalidade

Neto e Urban (2003) ressaltam que muitas estratégias com opções como, por exemplo, strangles e butterflies, apresentam as maiores perdas quando o ativo objeto pouco varia. Alguns modelos trabalham com cenários extremos e opostos, isto é, cenários de fortes altas ou fortes baixas. Desta forma, é necessário atentar para a existência de simulações que levem em consideração a não alteração no preço dos ativos.

### 7.2.3- Deslocamentos não paralelos da curva de juros

Deslocamentos não paralelos das estruturas a termos de taxas de juros. Neto e Urban (2003) ressaltam que as curvas de juros podem assumir uma grande quantidade de formas de movimentos: variação no nível, variação na inclinação, variação da curvatura e todas as combinações possíveis quando nível, inclinação e curvatura se alteram simultaneamente. Neste caso, é necessário a avaliar o tratamento do modelo para os diversos tipos de movimentos das curvas.

## 7.3- Back-test

O procedimento de avaliar um modelo é chamado de back-test ou teste retroativo, cujo objetivo é fornecer uma medida de validade do modelo de VaR utilizado. A avaliação estatística de um modelo para cálculo do VaR é efetuada, entre outros procedimentos, pela comparação entre o número de vezes que a série de retornos excedeu os limites de confiança (taxa de falhas) e a probabilidade nominal adotada no VaR.

O avaliador do risco de modelagem deve atentar para as limitações dos testes retroativos e, se necessário, sugerir testes complementares que validem com maior segurança os modelos.

### 7.3.1- Taxa e independência das falhas

O teste proposto por Kupiec (1995) é o mais adotado pelas instituições financeiras e consiste na comparação do valor nominal com o valor empírico da taxa de falhas. Contudo, esse tipo de teste, apesar de comumente utilizado, apresenta problemas devido a sua natureza incondicional, enquanto os intervalos de confiança são estimados condicionalmente.

Christoffersen (1998) ressalta que o problema de determinar a acurácia no cálculo do VaR deve considerar, além da correta taxa de falhas, a propriedade de independência dos erros. Esta condição coloca uma restrição de que forma as "violações" do VaR devem ocorrer. Especificamente, as violações devem ser

independentes entre si, ou seja, se uma violação prévia do VaR é um presságio de um próxima violação, então isso indica um erro no cálculo prévio do VaR.

Segundo Campbell (2005), um cálculo de VaR confiável deve apresentar tanto uma correta taxa de falhas, quanta a independência entre as falhas.

### 7.3.2- Base de avaliação do resultado

Outro fator a ser considerado na realização do back-test refere-se ao critério utilizado para comparação dos resultados. Neste contexto, segundo o Comitê da Basiléia (1996) as duas formas principais são: (a) comparação periódica do VaR diário das instituições financeiras com o subseqüente ganho ou perda do dia e (b) através da avaliação da sensibilidade da carteira estática às mudanças instantâneas nos preços dos ativos, ou seja, as posições do final do dia são registradas no sistema de risco, que calcula as possíveis mudanças no valor da carteira em função das mudanças de preços e taxas em um dado horizonte de tempo.

Segundo Campbell (2005) ambos os métodos apresentam argumentos prós e contras. Por exemplo, uma das linhas de raciocínio defende que o VaR não deve ser comparado contra resultados reais de ganhos e perdas, uma vez que esses resultados estarão, inevitavelmente, “contaminados” com as mudanças das posições na carteira ocorridas no horizonte de tempo. De acordo com essa visão, receitas como, por exemplo, prestação de serviços, que não estão ligadas ao resultado das operações da tesouraria e que não estão relacionadas à carteira estática que foi baseada o cálculo do VaR poderiam distorcer o resultado dos testes retroativos.

Ainda segundo Campbell (2005) existe outra linha de raciocínio que defende que os ganhos e perdas reais são as informações que mais importam para a instituição financeira e que a modelagem do VaR deve tomar essa medida como o benchmarking, mesmo que as premissas por trás sejam, de certa forma, limitadas. Adicionalmente, é argumentado que  problemas como, a receita de prestação de serviços, podem ser extraídos do resultado antes da realização do back-test.

Sendo assim, como ambos os procedimentos apresentam fatores positivos e negativos, segundo Campbell (2005) esta é a razão que o Comitê da Basiléia obriga os bancos a desenvolverem a capacidade de realizar testes retroativos utilizando tanto resultados hipotéticos quanto reais. O argumento seria que ambas as metodologias apresentam fatores positivos e, portanto, a combinação das duas formas é mais provável de gerar maior segurança na relação entre calcular o risco e o resultado das operações.

## 7.4- Apreçamento

O conceito fundamental aqui é a marcação-a-mercado. O risco de apreçamento é fortemente relacionado com o risco de modelagem.

Muitos modelos financeiros de apreçamento são baseados na teoria de não-arbitragem, onde os preços são determinados com base em outros preços cotados no mercado de uma forma tal que não é possível realizar operações de arbitragem.

Citamos como exemplo as seguintes condições de não arbitragens existentes em instrumentos financeiros:

Paridade de taxas de juros com os contratos futuros de juros;
Paridade put-call para opções européias;

Na avaliação do modelo de apreçamento utilizado pela instituição, é importante avaliar a existência da condição de não arbitragens dos modelos de apreçamento dos ativos. Apesar de sujeita à falhas, ainda é a condição mais aceita para apreçamento de ativos na teoria de finanças moderna.

A redução do risco de apreçamento passa por dois conceitos básicos, mas fundamentais para o processo: a independência na coleta de dados e uma boa metodologia de apuração do valor de mercado. O próprio Banco Central tem enfatizado que “a metodologia de apuração do valor de mercado é de responsabilidade da instituição e deve ser estabelecida com base em critérios consistentes e passíveis de

verificação, que levem em consideração a independência na coleta dos dados em relação às taxas praticadas em suas mesas de operações".

A situação ideal seria apreçar os ativos com base nas negociações realizadas entre os participantes do mercado. Contudo, o baixo nível de liquidez de determinados ativos faz com que os dados relativos a esse mercado sejam pouco representativos, sendo que muitos ativos não chegam a contabilizar sequer um único negócio por vários dias consecutivos.

Coelho, Macahyba e Bertolossi (2003) ressaltam que com o objetivo de reduzir as imperfeições existentes, a Andima, desde fevereiro de 2000 divulga taxas para negociação do mercado secundário para o conjunto de títulos públicos federais, exceto alguns com características específicas, como os créditos securitizados. As taxas médias são calculadas com base no envio de informações pelos participantes (*price makers*) e pela aplicação de metodologia específica para aplicação de filtros e interpolação de taxas.

Sendo assim, além do modelo, é fundamental observar as fontes de obtenção dos dados, atentando para a independência dos mesmos, sendo que para os ativos que são marcados a mercado através da observância dos valores, ou seja, sem a realização de cálculo com base em modelos matemáticos, a independência na coleta dos dados é questão fundamental.

Por outro lado, as Circulares 3.086/02 e 3.096/02 do Banco Central do Brasil, que tratam dos procedimentos para o registro e avaliação contábil de títulos e valores

mobiliários e a Circular 3.082/02 que trata dos procedimentos para registro e avaliação de instrumentos derivativos trouxeram profundas modificações nas regras existentes até então, obrigando as instituições financeiras a classificar os ativos financeiros de acordo com a estratégia de investimento.

Consequentemente, além da independência na obtenção dos dados e a qualidade do modelo matemático de apreçamento, a marcação a mercado deve incorporar uma terceira variável de risco que é a conformidade com as estratégias de investimentos.

Neste contexto, a marcação a mercado deve respeitar essas estratégias de investimentos, conforme estabelecido na legislação.

Em outubro de 2004 o colegiado da Comissão de Valores Mobiliários (CVM) condenou o Bank of America S/A CCVM a pagar multa de R$ 2 milhões por interromper os critérios de marcação a mercado durante um período de cerca de dez dias, no ano de 2002. As multas aplicadas refletem a punição máxima possível no caso em questão e foram determinadas por decisão unânime do Colegiado da autarquia. Fonte: Valor Econômico

## 8- Avaliação do Risco de Informação para Tomada de Decisão

Uma instituição financeira deve ser capaz de acessar as informações sobre sua condição e performance financeira de forma ampla, precisa, relevante e tempestiva. A disponibilidade das informações sobre a performance da instituição financeira é fundamental para avaliação dos resultados.

Adicionalmente, as informações devem ser enviadas aos efetivos responsáveis, especialmente a Alta Administração e acionistas.

Moreira (2003) menciona que existem sete categorias abrangentes de informação que devem ser abordadas pelos bancos na divulgação de seus relatórios, conforme demonstrado abaixo:

- Performance financeira;
- Posição financeira – capital, solvência e liquidez;
- Estratégias e práticas de gerenciamento de riscos;
- Exposições de riscos (crédito, mercado, liquidez, operacional, legal e outros riscos);
- Práticas contábeis;
- Principais negócios, gerência e governança corporativa;
- *Disclosure* no capital econômico.

A questão fundamental na avaliação desse risco passa pelo conceito de transparência, ou seja, de que forma e em que nível de profundidade, é possível os

acionistas, diretores, reguladores, credores e outros avaliarem e conhecerem da instituição.

No Novo Acordo da Basiléia essa preocupação é evidenciada de forma no Pilar 3 que trata do uso efetivo de uma “disciplina de mercado”para fortalecer a transparência do sistema bancário e incentivar o estabelecimento de práticas bancárias sólidas e seguras. Fato este que vem incentivando o Banco Central do Brasil a implementar diversas regulamentações que obrigam as instituições a divulgarem um número maior e mais complexo de informações.

Na avaliação da gestão do risco de prestação de informação, cabe ao avaliador conhecer os mecanismos de divulgação, incluindo os relatórios emitidos e suas respectivas informações, atentando para a qualidade das informações divulgadas e ao respectivo público das mesmas.

## 9- Avaliação da Gestão do Risco de Crédito

Duarte (2005) define o risco de crédito como o risco de perda decorrente da incapacidade ou da falta de disposição da contraparte em pagar suas obrigações. O risco de crédito ocorre em todas as atividades de negociação em que o resultado dependa da capacidade de pagamento de uma contraparte, de um emissor ou tomador.

Apesar do risco de crédito para a maioria das instituições ser a maior e mais óbvia fonte de risco, a avaliação da gestão do risco de crédito em uma instituição financeira com foco em operações de Tesouraria deve ser feita sob um prisma diferente da avaliação do risco de crédito "tradicional", uma vez que, neste perfil de instituição não é comum a existência da concessão de crédito tradicional.

Neste contexto, grande parte das operações de Tesouraria ocorre com instrumentos negociados em bolsa, em que a caixa de liquidação assume o risco de crédito da contraparte por meio de margens e contratos de liquidação por diferença. Esses contratos são utilizados para limitar a difusão de problemas de crédito ou de liquidez se empresas ou instituições específicas tiverem dificuldade para cumprir suas obrigações. Contudo, o risco de crédito se faz presente nas operações e deve ser monitorado corretamente.

O primeiro controle de uma instituição contra o risco excessivo de crédito é o processo inicial de concessão de crédito e, desta forma, é recomendável que as negociações não possam ser iniciadas até que seja aprovada uma linha de crédito para a contraparte. Os responsáveis pela avaliação de crédito e pela definição de limites

devem ser executivos de crédito independentes da função de tesouraria. Os padrões utilizados devem ser consistentes com aqueles utilizados para o estabelecimento de linhas de crédito tradicionais.

Para isso, é importante que a Alta Administração desenvolva uma política de crédito definindo estratégias e metas para a carteira de créditos, que serão utilizadas como base na aprovação dos limites de crédito, coerentes com a tolerância a risco da instituição.

Para avaliar a gestão do risco de crédito, é importante ter em mente que não deve basear-se puramente no valor referencial dos contratos. Instituições financeiras ativas em negociação devem calcular o risco de crédito pela adição da exposição positiva atual do contrato mais uma estimativa da potencial variação de valor ao longo do prazo restante do contrato. Uma abordagem menos sofisticada é avaliar o risco total de crédito pela multiplicação do valor referencial por uma porcentagem relacionada ao prazo do contrato.

Dentre as principais operações que apresentam risco de crédito, ressaltamos: operações de câmbio (interbancário, financeiro e pronto), aquisição de Eurobonds e títulos de dívida e operações com derivativos realizadas em balcão, tais como Swaps e Opções.

## 10- Risco Legal

Duarte (2005) define o risco legal como o risco relacionado a possíveis perdas quando um contrato não pode ser legalmente amparado, podendo-se incluir riscos de perdas por documentação insuficiente, insolvência, ilegalidade, falta de representatividade e/ou autoridade por parte de um negociador. Ainda segundo o autor, este risco engloba outros riscos, como o risco de legislação, tributário e de contrato.

A gestão do risco legal é um ponto extremamente importante e difícil de ser avaliado, especialmente quando essa avaliação não for realizada por um profissional com conhecimento específico, tais como, um auditor especialista em tributos ou um advogado. Isto porque não é raro encontrar questões de difícil tratamento, tais como:

- Regulamentações que se contrapõem;
- Ambigüidade na interpretação de legislação;
- Falta de clareza na formalização das regulamentações;
- Regulamentações que não dão suporte às regras do Banco Central do Brasil.

A seguir trataremos de algumas questões relevantes na avaliação da gestão desses riscos.

### 10.1 – Risco de legislação

Duarte (2005) define o risco de legislação como perdas potenciais impostas por regulamentação ou processos de clientes contra a instituição. A seguir

apresentaremos as principais questões a serem avaliadas no tratamento do risco de legislação.

Engloba a avaliação dos registros dos atos e livros societários ou de constituição legal da instituição. Neste contexto, Parada Filho (2006) menciona a obrigatoriedade de constituir os seguintes documentos:

- Livros contábeis e fiscais
- Livro Caixa
- Livro Diários
- Livro Razão
- LALUR – Livro de Apuração do Lucro Real
- Livro de inventário
- Livro de compras

Livros Societários instituídos pela Lei das Sociedade por Ações

- Registro de Ações Nominativas
- Transferência de Ações Nominativas
- Registro de Partes Beneficiárias Nominativas
- Atas das Assembléias Gerais
- Presença dos Acionistas
- Atas das Reuniões do Conselho de Administração\
- Atas das Reuniões de Diretoria
- Atas e Pareceres do Conselho Fiscal

Livros Trabalhistas

- Livro de Registro de Empregados
- Livro de Ponto
- Livro de Termos de Ocorrências Fiscais
- Folha de Pagamento
- Quadro de Horário
- Guias de Recolhimento à Previdência Social
- RAIS – Relação Anual de Informações Sociais
- DIRF – Declaração do Imposto de Renda Retido na Fonte
- Declaração do Imposto de Renda Pagos ou Creditados

Ainda dentro do conceito de risco de legislação, vale ressaltar a avaliação da conformidade sob os aspectos regulamentares específicos que permeiam as instituições financeiras.

Dentro deste contexto, é importante avaliar, pelo menos, a existência dos seguintes controles:

- Existência de controles sobre a identificação das alterações regulamentares, incluindo a forma e freqüência de identificação dos normativos emitidos pelos órgãos reguladores;
- Como a responsabilidade pelo atendimento a essas novas regulamentações é delegado aos funcionários, ou seja, como é definido quem são os responsáveis por fazer o que. Desta forma, reduzindo o risco de que as pessoas não façam o que deveriam fazer ou façam algo que não deveriam fazer;
- Como é monitorada a conformidade em relação à prestação de informações aos órgãos reguladores, ou seja, como os gestores se asseguram que as diversas

informações solicitadas pelos órgãos reguladores, especialmente o Banco Central do Brasil e a CVM, são repassadas de forma tempestiva, completa e íntegra;

- Verificação do nível de aprovação formal, incluindo a verificação independente por pessoa com alçada antes do envio das informações;

Tabela 11: Ordem de relevância na exposição dos riscos

| Posição | Risco |
|---|---|
| 1 | Regulamentação |
| 2 | Risco de Crédito |
| 3 | Corporate Governance |
| 4 | Derivativos |
| 5 | Hedge funds |
| 6 | Fraude |
| 7 | Risco de câmbio |
| 8 | Alta dependência em tecnologia |
| 9 | Técnicas de gerenciamento de risco |
| 10 | Tendências macroeconômicas |

Fonte: PricewaterhouseCoopers (2005)

## 10.2- Risco Tributário

Duarte (2005) define o risco tributário como perdas potenciais decorrentes da criação de novos tributos ou mudança na interpretação dos tributos existentes, sendo um risco extremamente relevante em qualquer instituição financeira.

Na avaliação da gestão do risco tributário, devem ser tratados de forma especial os aspectos relacionados às operações com derivativos. Isto porque não só são instrumentos financeiros muito utilizados pelas instituições, como também os aspectos regulamentares vem sofrendo mudanças profundas no Brasil e no mundo.

Santos (2004) menciona que devido à relativa singularidade das operações com derivativos, há ainda alguma dificuldade com a interpretação dos normativos e essa incerteza jurídica pode resultar em prejuízos inesperados e substanciais.

Essa incerteza passa por um ponto crítico na gestão do risco tributário que se refere à forma de classificação das operações financeiras, especialmente os instrumentos financeiros derivativos, como operações de hedge ou especulativa. Isto porque, de acordo com o artigo 27 da IN SRF 247, esta classificação será o ponto chave entre a possibilidade da instituição financeira compensar ganhos com perdas e, consequentemente, pagar menos tributos, especialmente PIS e Cofins.

Urge ressaltar que, na prática, para mitigar o risco de autuação fiscal perante a Secretaria da Receita Federal, é necessário que a instituição financeira atenda os requisitos do seu órgão regulador, no caso, o Banco Central do Brasil no que tange a

possibilidade de classificação das operações como *hedge*. Desta forma, trataremos a questão fiscal no que tange as operações de *hedge* a partir dos normativos do Banco Central do Brasil.

No Brasil o principal normativo emitido pelo Banco Central no que tange o registro e avaliação dos instrumentos financeiros derivativos é a Circular 3.082/02. Está definido nesta regulamentação que *hedge* é "a designação de um ou mais instrumentos financeiros derivativos com o objetivo de compensar, no todo ou em parte, os riscos decorrentes da exposição a variações no valor de mercado ou no fluxo de caixa de qualquer ativo, passivo, compromisso ou transação futura prevista, registrado contabilmente ou não, ou ainda grupos ou partes desses itens com características similares ou cuja resposta ao risco objeto de *hedge* ocorra de modo semelhante."

Ainda segundo o normativo, é necessário discriminar as operações em duas classes: *hedge* de risco de Mercado e *hedge* de risco de Fluxo de Caixa.

O mesmo normativo define que a contabilização deve reconhecer no mesmo resultado os efeitos compensatórios oriundos de modificações no valor justo dos instrumentos de *hedge* e dos itens *hedgeados*, com a indicação de que as variações no valor de mercado ou do fluxo de caixa do instrumento de *hedge* compensam as variações no valor de mercado ou do fluxo de caixa do item objeto de *hedge* num intervalo entre 80% e 125%.

Além da efetividade do *hedge*, o normativo define ainda outras condições necessárias para a classificação das operações como *hedge*, sendo elas:

- Possuir identificação documental do risco objeto de *hedg*e, com informação detalhada sobre a operação, destacados o processo de gerenciamento de risco e a metodologia utilizada na avaliação da efetividade do *hedge* desde a concepção da operação;
- Prever a necessidade de renovação ou de contratação de nova operação no caso daquelas em que o instrumento financeiro derivativo apresente vencimento anterior ao do item objeto de *hedge*;
- demonstrar, no caso dos compromissos ou transações futuras objeto de *hedge* de fluxo de caixa, elevada probabilidade de ocorrência e comprovar que tal exposição a variações no fluxo de caixa pode afetar o resultado da instituição;
- Não ter como contraparte empresa integrante do consolidado econômico-financeiro.

Urge ressaltar que, diante das diversas condições impostas para classificação das operações como *hedge*, as operações de "macro-*hedges*", que ocorrem quando diversas operações financeiras são realizadas com o objetivo de *hedgear* diversas outras operações financeiras de forma global e, portanto, sem uma ligação direta entra as operações não atendem aos requisitos de *hedge* do Banco Central do Brasil e, consequentemente, da Secretaria da Receita Federal.

Recentemente, a Boston Comercial e Participações Ltda., empresa do grupo Boston, foi autuada pela Receita Federal por ter remetido, em fevereiro de 1999, R$ 477 milhões ao exterior sem fazer a retenção de Imposto de Renda. A empresa havia

declarado que o valor se referia a pagamento por perdas em operação de hedge, o que livrava a remessa do IR. A autuação totaliza R$ 110,479 milhões, o que inclui multa de 75% e juros até abril de 2002.

A Receita concluiu que o pagamento não derivou de hedge, mas foi resultado de operações especulativas que envolveram o BankBoston NA Brasil e o BankBoston Banco Múltiplo, além da matriz norte-americana. A operação foi feita num período de crise cambial no qual o preço do dólar passou de R$ 1,21 em 12 de janeiro de 1999 para R$ 2,10 em 4 de março seguinte. Fonte: Valor Econômico.

O conceito fundamental é a transparência nas operações e nos controles da instituição financeira. Minha experiência como Gerente de Controles Internos em uma instituição financeira, é que, na prática, para uma operação ser considerada como hedge, e, consequentemente reduzir a carga tributária mitigando o risco fiscal, é a necessidade de se demonstrar a efetividade do hedge, através de controles internos e provas documentais, bem como a existência de uma premissa do que os auditores do Banco Central do Brasil convencionaram denominar "*hedge* contábil", ou seja, é necessário que o *hedge* financeiro seja identificado de forma clara através dos demonstrativos contábeis.

**10.3- Risco de Contrato**

Duarte (2005) o risco de contrato como perdas potenciais decorrentes de contratos omissos ou mal redigidos (sem o devido amparo legal).

A avaliação da gestão desse risco engloba a verificação da conformidade de, pelo menos, os seguintes controles:

- Existência de políticas que definam de forma clara os documentos necessários para realização de cada tipo de operação;
- Aprovação formal do Departamento Jurídico de todos os contratos antes da assinatura dos contratos;
- Avaliação dos controles sobre a verificação formal dos poderes de alçada das contrapartes com o objetivo de garantir que os contratos estejam bem representados;
- Avaliação da legitimidade da instituição praticar determinados atos previstos em lei e no seu estatuto social;

Em relação a legitimidade em praticar determinados atos previstos em leis, urge ressaltar a decisão tomada em 24/03/04 do Conselho de Recursos do Sistema Financeiro Nacional em aplicar multa no valor de R$100.000,00 ao Banco Prosper por realizar empréstimos com o fim de transferir recursos, indevidamente, a controlada indireta, afrontando a lei bancária, o que acabou por comprometer o bem jurídico tutelado em última análise pela norma que veda empréstimos entre pessoas ligadas.

## 11- Outros Riscos

A seguir apresentaremos outras questões que devem ser abordadas na avaliação dos controles internos:

### 11.1- Padrões éticos

Uma questão muitas vezes negligenciada, mas essencial, é a existência de um código de conduta para os funcionários, especialmente de Tesouraria. O código de conduta aumenta os controles sobre os padrões de honestidade e probidade que se esperam deles. O Manual de Supervisão do Banco Central menciona que esses padrões escritos devem abranger, pelo menos, os seguintes pontos:

- Negociação com entidades/subsidiárias da instituição ou com membros da Alta Administração;
- Negociação com outros funcionários da instituição;
- Negócios pessoais dos operadores nos mercados financeiros;
- Relacionamento pessoal com os corretores com os quais o banco opera;
- Negociações fora do expediente ou fora das instalações do banco;
- Aderência aos padrões e práticas éticas do mercado internacional.

### 11.2 – Política de Remuneração Variável

Neste contexto, muitas vezes as instituições definem padrões agressivos de remuneração variável para os funcionários da Tesouraria. Neste contexto, é importante avaliar se essa política de remuneração dos operadores e da equipe de

tesouraria não transmitem sinais conflitantes. Isto é, a Administração não deve endossar os controles de risco e ao mesmo tempo recompensar os operadores por seus resultados apenas de curto prazo com altas bonificações e, inclusive, não é recomendável que a remuneração de um operador dependa demais de metas individuais uma vez que metas agressivas podem forçar os operadores a assumir posições excessivas e arriscadas ou a ocultar perdas. Adicionalmente, é recomendável que os bônus sejam baseados no desempenho ajustado pelo risco.

**11.3- Segregação de funções**

A experiência do "caso Barings" demonstra a importância da existência de segregação de função dado que uma das principais falhas identificadas foi à ausência de monitoramento independente dos seus limites operacionais.

Para obter um sistema de controles internos apropriado é necessário que as atividades de aprovação de limites, registro, monitoramento e liquidação das transações da tesouraria, sejam segregadas e gerenciadas de forma independente da mesa de operações. Neste contexto, deve ser avaliado se o pessoal da mesa de operações está envolvido com as atividades de confirmação de transações, reavaliação de posições, lançamentos contábeis, autorizações de desembolso de fundos ou solução de disputas envolvendo operações.

A área de "back-office"é quem deve detectar os erros e leva-los à atenção dos operadores e da Alta Administração. A estrutura do back-office pode variar ou mudar

segundo os volumes e produtos. No entanto, a unidade deve se reportar a Alta Administração, fora da função de negociações, para que esta esteja ciente dos principais riscos operacionais.

**11.4 – Registro e formalização das operações**

O fluxo das operações entre o "front-office", o "middle-office" e "back-office" pode envolver processos manuais e completamente computadorizados. Não obstante, é importante avaliar que se os procedimentos possuem, entre outros, os seguintes controles nos boletos das operações:

- Identificação por número seqüencial, data e hora;
- Responsáveis pela aprovação, efetivação e conferência;
- Contrapartes;
- Instrumento, preço, montante e prazo;
- Despesas de corretagens e comissões;
- Valores de margens

Idealmente, os boletos seriam inseridos em um sistema automaticamente que alimentasse uma base de dados centralizados que, a partir de interfaces com os sistemas de gestão de riscos seriam feito os controles dos limites operacionais estabelecidos. Esse processo é comumente chamado de "boletamento único".

Outro aspecto essencial refere-se a documentação da estratégia da operação. Não só as "boas práticas operacionais", como também o Banco Central do Brasil,

através das Circulares 3.082 e 3.068 tornaram essencial a identificação da estratégia das operações.

Neste contexto, devem existir políticas claras e formalmente estabelecidas que especifiquem a forma e o conteúdo da documentação necessária para atender às exigências regulamentares, especialmente as que se referem às estratégias de *hedge*. Os seguintes pontos devem ser atentados:

- A contabilização de *hedge* é utilizada para transações de derivativos, quando apropriadas;
- Transações de derivativos não qualificados como "contabilização de *hedge*" são marcados a mercado;
- Verificar a documentação dos hedge para determinar se eles estão razoavelmente ligados aos ativos ou passivos que se destinam a proteger

**11.5- Confirmação das operações**

Após os registros dos boletos nos sistemas corporativos, as operações devem ser confirmadas com as contrapartes com o objetivo de verificar se cada uma das contrapartes concordam com os termos da operação. Para reduzir o potencial de fraude ou de falha humana, a unidade de processamento deve iniciar, acompanhar e controlar todas as confirmações das contrapartes, sendo que as não conformidades devem ser identificadas o mais breve possível, investigadas de forma independente e reportadas a Alta Administração, de forma a garantir que sejam obtidas novas

confirmações para alterações nos termos acordados. Quaisquer alterações devem ser reportadas aos operadores e lançadas corretamente em seus bancos de dados oficiais.

### 11.6- Liquidação das operações

Liquidação é o processo pelo qual as operações são compensadas pelo pagamento/recebimento de moeda, títulos ou fluxos de caixa em datas de pagamento periódicas ou finais. Nesta etapa é importante que os funcionários responsáveis pelo caixa sejam independentes daqueles que executam, aprovam ou contabilizam as operações, sendo necessário avaliar a quantidade de liquidações em atraso e justificativa dos motivos.

### 11.7- Procedimentos de conciliação

Para assegurar que todas as transações sejam adequadamente contabilizadas, a área de back-office deve executar conciliações periódicas, de acordo com as políticas e os procedimentos pré-estabelecidos. As reconciliações devem ser revisadas e formalmente aprovadas. É recomendável a existência de conciliação, no mínimo, dos seguintes relatórios:

- Registro gerencial dos operadores com o sistema operacional;
- Sistema operacional com o sistema contábil;
- Sistema contábil com as câmaras de compensação (CBLC, BM&F, Selic, Cetip, etc..)

- Sistema operacional com os relatórios das corretoras;
- Sistema operacional com os sistemas de gerenciamento de riscos;
- Performance dos operadores com a conta de lucros e perdas gerenciais;
- Sistema contábil com os relatórios de envio aos órgãos reguladores;

**11.8- Conflito de interesse**

O conflito de interesse está intimamente ligado ao risco de fraude, surgindo quando o funcionário tem algum grau de parentesco, amizade ou interesse financeiro na transação, a qual pode dividir seus interesses e, desse modo, trazer prejuízo a instituição.

Ao se avaliar o nível existente de conflito de interesse na instituição, devem ser atentados, no mínimo, os seguintes pontos de controle:

- Segregação de tarefas entre as áreas de front-office, middle-office e back-office;
- Verificação da existência de contas suspeitas, tal como, a “conta erro”;
- Política de escolha de corretora, garantindo que as operações sejam intermediadas pelas corretoras que oferecem, de fato, os melhores serviços. Essa política deve ser acompanhada, idealmente, por um processo de *due dilligence*.
- Monitoramento do risco de *churning*, ou seja, realização de troca de posições em carteira que não são justificadas por informações e fundamentos e possuem como único objetivo, a realização de despesas de corretagem incorridas para atender o benefício pessoal do operador;

- Normas para realização de investimentos pessoais, atentando para as restrições e monitoramento das operações realizadas na carteira própria dos operadores e familiares;

Se possível, obrigar a concentração da realização das operações na carteira própria dos funcionários em uma única corretora que, posteriormente, envia as operações à área de Compliance para q respectiva avaliação das mesmas;

- Alto índice de cancelamento de boletas sem justificativas plausíveis;
- Realização de *front-running*, ou seja, realização de operação com base em informação não pública e antecipando aos movimentos de mercado;
- Não possibilitar o uso de telefones celulares na mesa de operações e garantir que todas as ligações sejam gravadas;
- Funcionários com férias vencidas e não gozadas;
- Revisar a política de escolha de fornecedores, incluindo a existência, quando possível, de mapa de cotação ou, alternativamente, documentar a escolha de determinados fornecedores;
- Política de aceitação de brindes e incentivos;

## 12. Conclusão

O sistema de controles internos, à medida que desempenha funções relevantes no mundo atual, é necessário que sejam constantemente avaliados de forma eficiente. Essa avaliação é uma necessidade imposta não só por àqueles que buscam a eficácia organizacional, como também pelos próprios órgãos reguladores.

Neste contexto, o sistema de controles internos deve ser desenhado de forma a comprovar sua eficácia, ou seja, não basta ser eficaz, é necessário comprovar de forma clara, através da devida documentação, essa eficácia. Isto porque um sistema de controles internos que não esteja apoiado em processos de avaliações que evidenciem a mitigação dos riscos, pode ser considerado, de certa forma, inútil, uma vez que não é possível confiar plenamente no mesmo.

É claro que confiar nos gestores é algo extremamente relevante para a Alta Administração, porém é necessário reconhecer que essa atitude envolve riscos e que a história possui diversos exemplos que comprovam que apenas confiar nos gestores não é a decisão mais eficiente.

O processo de avaliação dos controles internos por pessoa independente e capacitada deve ser encarado como algo complementar e não somente por algo imposto pelos órgãos reguladores.

Os responsáveis pelo processo de avaliação dos controles internos, geralmente os auditores e compliance officers, são fundamentais e estes por sua vez, devem estar

atentos aos riscos inerentes à gestão dos processos. Trata-se de um braço estratégico extremamente importante que auxilia diretamente no gerenciamento efetivo dos riscos da instituição.

## Anexos

### Anexo 1 - Princípios Essenciais para uma Supervisão Bancária Eficaz – Basle Committee on Banking Supervision

#### Pré-condições para uma Supervisão Bancária Eficaz

1. Um sistema eficaz de supervisão bancária terá claramente definidas as responsabilidades e os objetivos de cada agência envolvida na supervisão de organizações bancárias. Cada uma dessas agências devem ter independência operacional e recursos adequados. Um ordenamento legal apropriado à supervisão bancária também é necessário, incluindo dispositivos relacionados com as autorizações às organizações bancárias e sua supervisão contínua; poderes voltados para a verificação de conformidade legal, bem como para interesses de segurança e solidez; e proteção legal para os supervisores. Também devem ser contemplados dispositivos referentes à troca de informações entre supervisores e à proteção da confidencialidade de tais informações.

#### Autorizações e Estrutura

2. As atividades permitidas às instituições autorizadas a operar como bancos, sujeitas à supervisão, devem ser claramente definidas e o uso da palavra “banco” nos nomes das instituições deve ser controlado na medida do possível.

3. O órgão autorizador deve ter o direito de estabelecer critérios e de rejeitar pedidos de autorização para operação que não atendam aos padrões exigidos. O processo de autorização deve consistir, no mínimo, de uma avaliação da estrutura de propriedade da organização bancária, seus diretores e principais administradores, seu plano operacional e seus controles internos, e suas condições financeiras projetadas,

inclusive a estrutura de capital. Quando o proprietário ou controlador da instituição proponente for um banco estrangeiro, deve-se condicionar a autorização a uma prévia anuência do órgão supervisor do país de origem.

4. Os supervisores bancários devem ter autoridade para examinar e rejeitar qualquer proposta de transferência significativa, para terceiros, do controle ou da propriedade de bancos existentes.

5. Os supervisores bancários devem ter autoridade para estabelecer critérios para exame das aquisições e dos investimentos mais relevantes de um banco, assegurando que as estruturas e ramificações corporativas não exponham o banco a riscos indevidos, nem impeçam uma supervisão eficaz.

**Regulamentos e requisitos prudenciais**

6. Os supervisores bancários devem estabelecer, para todos os bancos, requisitos mínimos, prudentes e apropriados, de adequação de capital. Tais requisitos devem refletir os riscos a que os bancos se submetem e devem definir os componentes de capital, levando em conta a capacidade de absorção de perdas de cada um. Pelo menos para os bancos com atuação internacional, esses requisitos não devem ser menos rigorosos do que os estabelecidos no Acordo de Capital da Basiléia.

7. Um elemento essencial de qualquer sistema de supervisão é a avaliação das políticas, práticas e dos procedimentos de um banco, relacionados com a concessão de empréstimos e com as decisões de investimento, bem como com as rotinas de administração de suas carteiras de crédito e de investimento.

8. Os supervisores bancários devem se assegurar de que os bancos estabelecem e cumprem políticas, práticas e procedimentos adequados à avaliação da qualidade de

seus ativos e para adequação de suas provisões e de suas reservas para perdas em operações de crédito.

9. Os supervisores bancários devem se assegurar de que os bancos adotam sistemas de informações gerenciais que possibilitem a identificação, pelos administradores, de concentrações dentro de suas carteiras. Os supervisores devem estabelecer limites que restrinjam a exposição dos bancos a tomadores individuais de crédito ou a grupos de tomadores inter-relacionados.

10. Visando prevenir abusos decorrentes de concessão de crédito a empresas e/ou indivíduos ligados ao banco concedente, os supervisores bancários devem estabelecer critérios que assegurem um rígido controle de tais operações, para que sejam efetivamente monitoradas. Outras medidas apropriadas devem ser adotadas para controlar ou reduzir os riscos inerentes a tais operações.

11. Os supervisores bancários devem se assegurar de que os bancos adotam políticas e procedimentos adequados para identificar, monitorar e controlar riscos de pais e riscos de transferência em suas atividades de empréstimo e de investimento internacionais, e para manter reservas apropriadas contra tais riscos.

12. Os supervisores bancários devem se assegurar de que os bancos mantêm sistemas que avaliam com precisão, monitoram e controlam adequadamente os riscos de mercado; os supervisores devem ter poderes para impor limites específicos e/ou um encargo específico de capital sobre exposições a riscos de mercado, se necessário.

13. Os supervisores bancários devem se assegurar de que os bancos adotam um processo abrangente de administração de risco (incluindo a supervisão adequada pelo Conselho de Diretores e pela Administração Sênior), para identificar, medir, monitorar e controlar todos os demais riscos materiais e, quando necessário, para manter capital contra tais riscos.

14. Os supervisores bancários devem determinar que os bancos mantenham controles internos adequados para a natureza e para a escala de seus negócios. Os instrumentos de controle devem incluir disposições claras para a delegação de competência e responsabilidade; a separação de funções que envolvem a assunção de compromissos pelo banco, a utilização de seus recursos financeiros e a responsabilidade por seus ativos e passivos; a reconciliação de tais processos; a proteção de seus ativos; e as funções apropriadas de auditoria e de conformidade independentes, internas ou externas, para verificar a adesão a tais controles, assim como às leis e regulamentos aplicáveis.

15. Os supervisores bancários devem determinar que os bancos adotem políticas, práticas e procedimentos, incluindo regras rígidas do tipo “conheça-seu-cliente”, que promovam elevados padrões éticos e profissionais no setor financeiro e previnam a utilização dos bancos, intencionalmente ou não, por elementos criminosos.

**Métodos de Supervisão Bancária Contínua**

16. Um sistema de supervisão bancária eficaz deve consistir da combinação de atividades de supervisão direta (in loco) e indireta.

17. Os supervisores bancários devem manter contato regular com as administrações dos bancos e conhecer profundamente todas as operações das instituições bancárias.

18. Os supervisores bancários devem dispor de meios para coletar, examinar e analisar relatórios prudenciais e estatísticos dos bancos, em bases individuais e consolidadas.

19. Os supervisores bancários devem dispor de meios para validação independente das informações pertinentes à supervisão, seja por intermédio de inspeções diretas, seja pelo uso de auditores externos.

20. Um elemento essencial da supervisão bancária é a capacidade de supervisionar grupos ou conglomerados bancários em bases consolidadas.

**Requisitos de Informação**

21. Os supervisores bancários devem se assegurar de que cada banco mantém registros adequados, definidos de acordo com políticas e práticas contábeis consistentes, que possibilitem uma avaliação precisa da real condição financeira do banco e da lucratividade de seu negócio, e de que os bancos publicam regularmente relatórios financeiros que reflitam com fidelidade suas condições.

**Poderes Formais dos Supervisores**

22. Os supervisores bancários devem dispor de meios para adotar ações corretivas oportunas quando os bancos deixarem de cumprir requisitos prudenciais (como índices mínimos de adequação de capital), quando houver violação de regulamentos ou quando, de alguma outra forma, houver ameaça para os depositantes. Para circunstâncias extremas, deve-se incluir a competência para revogar a autorização de funcionamento da instituição, ou para recomendar sua revogação.

**Atividades Bancárias Internacionais**

23. Os supervisores bancários devem realizar supervisão global consolidada nas instituições que atuam internacionalmente, monitorando adequadamente e aplicando normas prudenciais adequadas em todos os seus negócios de alcance mundial, principalmente suas filiais estrangeiras, joint-ventures e subsidiárias.

24. Um elemento chave da supervisão consolidada é o estabelecimento de contatos e o intercâmbio de informações com os vários outros supervisores envolvidos, principalmente as autoridades supervisoras do país hospedeiro.

25. Os supervisores bancários devem requerer que as operações locais de bancos estrangeiros sejam conduzidas com o mesmo padrão de exigência requerido das instituições locais e devem ter poderes para fornecer informações requeridas por autoridades supervisoras do país de origem, visando possibilitar-lhes a supervisão consolidada.

**Anexo 2 - 13 Princípios para a avaliação de sistemas de controles internos – Basle Committee on Banking Supervision**

**Controle pela administração e cultura de controle**

1. O Conselho de Diretores deve responsabilizar-se pela aprovação das estratégias e políticas; compreender os riscos incorridos pelo banco, ajustando-os a níveis aceitáveis e assegurando-se de que a Alta Administração tome as medidas necessárias para identificar, monitorar e controlar estes riscos; aprovação da estrutura organizacional; e assegurar-se de que a administração sênior monitora a eficácia do sistema de controles internos.

2. A administração sênior deve ter a responsabilidade de executar as estratégias aprovadas pelo conselho; ajustando as políticas internas apropriadas de controle; e monitorando a eficácia do sistema de controles internos.

3. O conselho de diretores e a administração sênior são responsáveis pela promoção de elevados padrões éticos e de integridade, e por estabelecer uma cultura dentro da organização que enfatiza e demonstra a todos os níveis do pessoal a importância dos controles internos. Todos os níveis do pessoal em uma organização bancária necessitam compreender seu papel no processo de controles internos e estar inteiramente engajados no processo.

**Avaliação de risco**

4. A administração sênior deve assegurar-se de que os fatores internos e externos que poderiam afetar adversamente a realização dos objetivos do banco estão sendo identificados e avaliados. Esta avaliação deve cobrir todos os vários riscos que o banco enfrenta (por exemplo, o risco de crédito, o risco do país e de transferência, o

risco de mercado, o risco de taxa de juros, o risco de liquidez, o risco operacional, o risco legal e o risco de reputação).

5. A administração sênior deve assegurar-se de que os riscos que afetam a realização das estratégias e de objetivos do banco estejam sendo continuamente avaliados. Os controles internos podem demandar revisão de modo a abranger apropriadamente novos riscos ou riscos previamente não controlados.

**Atividades de controle**

6. As atividades de controle devem ser uma parte integral das operações diárias de um banco. A administração sênior deve estabelecer uma estrutura apropriada de controle para assegurar controles internos eficazes, definindo as atividades de controle em cada nível do negócio. Estes devem incluir: revisões de alto nível; controles apropriados da atividade de departamentos ou divisões diferentes; controles físicos; verificação periódica de aderência aos limites de exposição; um sistema das aprovações e autorizações; e, um sistema da verificação e reconciliação. A administração sênior deve periodicamente assegurar-se de que todas as áreas do banco estejam aderentes às políticas e procedimentos estabelecidos.

7. A administração sênior deve assegurar-se de que existe segregação de funções apropriada e que ao pessoal não foram atribuídas responsabilidades conflitantes. As áreas de conflitos de interesse potenciais devem ser identificadas, minimizadas, e com cuidado ser monitoradas.

**Informação e comunicação**

8. A administração sênior deve assegurar-se de que existem dados financeiros, operacionais e de compliance internos adequados e detalhados, assim como

informação do mercado externa sobre os eventos e as circunstâncias que são relevantes ao processo de tomada de decisão. A informação deve ser confiável, oportuna, acessível, e disponibilizada em um formato consistente.

9. A administração sênior deve estabelecer canais efetivos de comunicação para assegurar-se de que toda a equipe de funcionários esteja inteiramente ciente das políticas e dos procedimentos que afetam seus deveres e responsabilidades e que outras informações relevantes estejam alcançando o pessoal apropriado.

10. A administração sênior deve assegurar-se de que existem sistemas de informação apropriados em funcionamento que cobrem todas as atividades do banco. Estes sistemas, incluindo aqueles que mantêm ou que se utilizam de dados em formato eletrônico, devem ser seguros e testados periodicamente.

**Monitoramento**

11. A administração sênior deve monitorar continuamente a eficácia total dos controles internos do banco, a fim de auxiliar no atendimento dos objetivos da organização. O monitoramento dos riscos chaves deve ser parte das operações diárias do banco e deve incluir avaliações independentes, de acordo com o caso.

12. Deve existir uma auditoria interna ampla e eficaz do sistema de controles interno realizado composto por funcionários apropriadamente treinados e competentes. A auditoria interna, como a parte do monitoramento do sistema de controles internos, deve reportar-se diretamente ao conselho de diretores ou ao comitê de auditoria, e à administração sênior.

13. As deficiências identificadas nos controles internos devem ser relatadas de forma tempestiva ao nível apropriado da administração e ser cuidadas prontamente. As

deficiências relevantes nos controles internos devem ser relatadas à administração sênior e ao conselho de diretores.

**Anexo 3 – Histórico das atividades de Compliance - GRUPO DE TRABALHO ABBI/FEBRABAN (2004)**

**1929** – Quebra da Bolsa de New York, Política Intervencionista "*New Deal*" – Governo do Presidente Teodore Roosevelt;

**1930 –** Criação de **Organismos de Controle** do Governo Federal Americano;

**1933/34 –** Diversos acontecimentos importantes:

- Congresso Americano vota medidas com vistas a **proteger** o mercado de títulos de valores mobiliários e seus investidores – ***Securities Act***;
- Criação da **SEC – Securities and Exchange Commission;**
  - ✓ *Exigência de registro do prospecto de emissão de títulos e valores mobiliários.*

**1940 –** *Investment Advisers Act* (registro dos consultores de investimento) e *Investment Company Act* (registro de fundos mútuos);

**1945 –** Conferências de Bretton Woods – Criação do Fundo Monetário Internacional e do BIRD, com o objetivo básico de zelar pela estabilidade do Sistema Monetário Internacional;

**1950 –** *Prudential Securities* – contratação de advogados para **acompanhar a legislação** e **monitorar** atividades com valores mobiliários;

**1960 – ERA COMPLIANCE;**

A **SEC** passa a insistir na contratação de ***Compliance Officers***, para:

- ***Criar Procedimentos Internos de Controles;***
- ***Treinar Pessoas;***
- ***Monitorar, com o objetivo de auxiliar as áreas de negócios a ter a efetiva supervisão.***

**1970 –** Desenvolvimento do Mercado de Opções e Metodologias de *Corporate Finance, Chinese Walls, Insider Trading, etc.*

**1974 –** O Mercado Financeiro Mundial apresenta-se perplexo diante do caso Watergate, que demonstrou a fragilidade de controles no Governo Americano;

**1974 –** Criação do Comitê da Basiléia para Supervisão Bancária;

**1980 –** A atividade de Compliance se expande para as demais atividades financeiras no Mercado Americano;

**1988 –** Foi estabelecido o Primeiro Acordo de Capital da Basiléia, estabelecendo padrões para a determinação do Capital mínimo das Instituições Financeiras.

**1988 -** A Convenção das Nações Unidas contra o Tráfico Ilícito de Entorpecentes e de Substâncias Psicotrópicas, Viena;

**1990 -** As 40 recomendações sobre lavagem de dinheiro da Financial Action Task Force - ou Grupo de Ação Financeira sobre Lavagem de Dinheiro (GAFI/FATF) - revisadas em 1996 e referidas como Recomendações do GAFI/FATF;

**1992 -** Elaboração pela Comissão Interamericana para o Controle do Abuso de Drogas (CICAD) e aprovação pela Assembléia Geral da Organização dos Estados Americanos (OEA) do "Regulamento Modelo sobre Delitos de Lavagem Relacionados com o Tráfico Ilícito de Drogas e Outros Delitos Graves";

**1995** – Importantes acontecimentos e mudança das regras prudenciais:

- ✓ A fragilidade no Sistema de Controles Internos leva à falência o **Banco Barings;**
- ✓ **Basiléia I** – Publicação de Regras Prudenciais para o Mercado Financeiro Internacional.

**1995 -** Criação do Grupo de Egmont com o objetivo de promover a troca de informações, o recebimento e o tratamento de comunicações suspeitas relacionadas à lavagem de dinheiro provenientes de outros organismos financeiros;

**1996 -** Complementado o Primeiro Acordo de Capital de 1988 para inclusão do Risco de Mercado dentro do cálculo do Capital Mínimo definido em 1988 pelo Comitê de Supervisão Bancária da Basiléia.

**1997 -** Divulgação pelo Comitê da Basiléia dos **25 princípios** para uma Supervisão Bancária Eficaz, com destaque para seu **Princípio de n.º 14:** *"Os supervisores da atividade bancária devem certificar-se de que os bancos tenham controles internos adequados para a natureza e escala de seus negócios. Estes devem incluir arranjos claros de delegação de autoridade e responsabilidade: segregação de funções que envolvam comprometimento do banco, distribuição de seus recursos e contabilização de seus ativos e obrigações; reconciliação destes processos; salvaguarda de seus ativos; e funções apropriadas e independentes de Auditoria Interna e Externa e de* ***Compliance*** *para testar a adesão a estes controles, bem como a leis e regulamentos aplicáveis".*

**1998 – Sistemas de Controles Internos**

- ✓ ***Basiléia*** – publicação dos **13 Princípios** concernentes a Supervisão pelos Administradores e Cultura / Avaliação de **Controles Internos**, tendo como fundamento a:

- ***Ênfase na necessidade de Controles Internos efetivos;***
- ***Promoção da estabilidade do Sistema Financeiro Mundial.***

✓ ***Banco Central do Brasil – publicação da Lei 9613/98***, que dispõe sobre crimes de lavagem ou ocultação de bens, a prevenção da utilização do Sistema Financeiro Nacional para atos ilícitos previstos na referida lei e cria o Conselho de Controle de Atividades Financeiras (COAF);

✓ ***Banco Central do Brasil*** – com base na publicação dos 13 Princípios concernentes a Supervisão pelos Administradores e Cultura / Avaliação de Controles Internos, publicou a **Resolução n.º 2554/98,** que dispõe sobre a implantação e implementação de sistema de controles internos, todavia ***não normatizou a função de Compliance;***

✓ ***Inicio de estudos sobre o Basiléia II – Regras Prudenciais;***

✓ *Declaração Política e o Plano de Ação contra Lavagem de Dinheiro, adotados na Sessão Especial da Assembléia Geral das Nações Unidas sobre o Problema Mundial de Drogas, Nova Iorque.*

**2001 –** Falha nos Controles Internos e Fraudes Contábeis levam a ENRON à falência;

**2001 -** US Patriot Act

**2002 –** Falha nos Controles Internos e Fraudes Contábeis levam à concordata da WORLDCOM;

**2002 – *Congresso Americano*** publica o "**Sarbanes-Oxley Act**", que determinou às empresas registradas na SEC a adoção das melhores práticas contábeis, independência da Auditoria e criação do Comitê de Auditoria;

**2002 -** Criação do GAFISUD;

**2002 -** Resolução 3056 do CMN que altera a resolução 2554 dispondo sobre a atividade de Auditoria sobre Controles Internos

**2003 – *Banco Central do Brasil*** - Publicação da **Resolução n.º 3.081** que trata da auditoria independente e regulamenta a instituição do ***Comitê de Auditoria***, com funções semelhantes àquelas publicadas pelo "**Sarbanes-Oxley Act**", devendo inclusive pronunciar-se sobre o quanto, emanado pela **Resolução n.º 2554/98** .

**2003 – *Comitê de Supervisão Bancária da Basiléia* –** Práticas recomendáveis para Gestão e Supervisão de Riscos Operacionais.

## Apêndice 1 – Guia rápido de perguntas

### Ambiente de Informática

1. A instituição possui plano estratégico de Tecnologia da Informação?
2. Os planos incorporam  indicadores de desempenho e metas?
3. Existência de um modelo de arquitetura de informações, abrangendo o modelo de dados corporativo e os sistemas de informação associados?
4. Existe uma divisão de tarefas entre as seguintes funções:
   - Uso de sistemas de informação;
   - Inserção de dados;
   - Operação de computadores;
   - Gerenciamento de rede;
   - Administração de sistemas;
   - Desenvolvimento e manutenção de sistemas;
   - Gerenciamento de alterações;
   - Administração de segurança;
   - Auditoria de segurança.
5. Todos os ativos relacionados a informações (dados e sistemas) tem um proprietário que tome decisões sobre sua classificação e direitos de acesso?
6. Existem políticas e procedimentos para controlar as atividades de consultores e outras pessoas contratadas pela área de TI para assegurar a proteção dos ativos relacionados a informações da organização?
7. Existe uma política de segurança que defina a abordagem geral da organização?
8. Essa política de segurança especifica o propósito e objetivos, o escopo dentro da organização, a definição e atribuição de responsabilidades para implementação em

todos os níveis e a definição de penas e ações disciplinares associadas à não-conformidade com as políticas de segurança e controles internos?

9. Existe um programa de conscientização de segurança em TI que comunica as políticas de segurança de TI para cada usuário e assegura um entendimento total da importância de tal segurança?
10. É definido a estrutura geral de gestão de projetos com escopo e limites para gerenciar projetos assim como a metodologia de gerenciamento a ser adotada e aplicada a cada projeto?
11. A alta administração revisa os relatórios dos estudos de viabilidade relevantes como base para sua decisão de como proceder com o projeto?
12. Existe um plano para a revisão da pós implementação de cada sistema de informação novo ou modificado para determinar se o projeto teve os benefícios planejados?
13. Existem mecanismos adequados de trilhas de auditoria para os sistemas?
14. São preparados manuais de apoio e de referência para usuários (preferivelmente em formato eletrônico) como parte de cada projeto de desenvolvimento ou modificação de sistemas?
15. As mudanças são testadas de acordo com o impacto e avaliação de recursos em um ambiente de teste separado por um grupo de teste independente (criadores) antes do início do uso no ambiente operacional regular?
16. Todas as solicitações de alterações, manutenção de sistema e manutenção de fornecedor são padronizadas e sujeitas a procedimentos formais de administração de mudança?
17. Os solicitantes de alterações são mantidos informados sobre o status de sua solicitação?

18. Existem acordos formais de níveis de serviços e conteúdo mínimo: disponibilidade, confiabilidade, desempenho, capacidade de crescimento, níveis de suporte oferecidos aos usuários, planejamento de continuidade, segurança, nível mínimo de satisfação com a funcionalidade do sistema, taxas de serviço e procedimentos de alterações?
19. Existe um processo de revisão regular para acordos de nível de serviço e contratos com outros fornecedores de serviços?
20. Existe um processo que define que antes da seleção, os fornecedores são apropriadamente qualificados através de uma avaliação de sua capacidade em prover os serviços necessários (due diligence)?
21. Existe um plano por escrito contendo:

    - Diretrizes sobre como usar o plano de continuidade ;

    - Procedimentos de emergência;

    - Procedimentos de resposta direcionados a recuperar o nível de negócios antes do incidente ou de ocorrências graves;

    - Procedimentos para salvaguardar e reconstruir o local de trabalho;

    - Procedimentos de coordenação com autoridades públicas;

    - Procedimentos de comunicação com acionistas, funcionários principais clientes e fornecedores, quotistas e administração;

    - Informação crítica sobre as equipes de continuidade, a equipe envolvida, clientes, fornecedores, autoridades públicas e a mídia
22. Existem procedimentos de controle de alterações a fim de assegurar que o plano de continuidade esteja atualizado e que possa refletir os requisitos reais do negócio?

23. As partes envolvidas recebem treinamento regular com relação aos procedimentos a serem seguidos no caso de um incidente ou ocorrência grave?
24. Os recursos de back-up são armazenados fora do local de trabalho e são periodicamente avaliados, pelo menos uma vez ao ano, com relação à proteção de conteúdo, ambiente e segurança?
25. Existem procedimentos para garantir ações tempestivas com relação a solicitação, definição, emissão, suspensão e cancelamento de contas de usuários que incluem procedimento formais de aprovação destacando os dados ou proprietário de sistemas garantindo os privilégios de acesso?
26. Existem procedimentos para manter ativos os mecanismos de acesso e autenticação (por exemplo, alterações de senha regulares)?
27. As atividades de segurança são registradas e qualquer indicação de violação iminente de segurança é relatada imediatamente a todos os interessados, interna ou externamente?
28. Os dados de transações importantes só são trocados em caminhos protegidos?
29. Existem medidas de controle preventivas, de detecção e corretivas e resposta a ocorrências e métodos de reportagem com relação a software destrutivo, tal como vírus de computador ou Cavalos de Tróia?
30. Existem firewalls adequados para proteção contra negação de serviços e qualquer acesso não-autorizado aos recursos internos?
31. Existem procedimentos para garantir que os documentos fonte sejam retidos ou que sejam reproduzidos pela organização por um período de tempo adequado para facilitar a recuperação ou reconstrução de dados e também para satisfazer requisitos legais?

32. São definidos os períodos de retenção e condições de armazenagem para documentos, dados, programas, relatórios e mensagens (de entrada e saída), assim como os dados (chaves, certificados) usados para sua criptografia e autenticação?
33. Existem medidas suficientes para a proteção contra fatores ambientais (por exemplo, incêndio, pó, eletricidade, calor excessivo e umidade). Instalar equipamentos e dispositivos especializados para monitorar e controlar o ambiente.

**Risco de Mercado**

1- É mantido de forma adequadamente documentada os critérios e a estrutura estabelecidos para o controle do risco de mercado?

2- Existem limites de exposição de risco de mercado, incluindo:

- Value-at-Risk;

- Stop-loss;

- Liquidez;

- Individuais;

- Stress

3- Os limites estão aprovados pela Alta Administração?

4- Os limites são monitorados de forma independente da mesa de operações?

5- Existem relatórios que permitam o monitoramento dos riscos de mercado assumido emitidos para a Alta Administração?

6- Os limites são monitorados em “tempo-real” de forma que não conformidades sejam identificadas a tempo, ou seja, de forma preventiva e não detectiva?

7- Como são tratadas as não conformidades? A Alta Administração é informada formalmente e de forma tempestiva?

**Risco de Liquidez**

1- É mantido de forma adequadamente documentada os critérios e a estrutura estabelecidos para o controle do risco de liquidez?

2- São elaboradas análises econômico-financeiras que permitam avaliar o impacto dos diferentes cenários na condição de liquidez de seus fluxos de caixa, levando em consideração, inclusive, fatores internos e externos à instituição?

3- A análise do fluxo de caixa permite, entre outros:

- Disponibilização de fluxos de caixa distintos por produto ou mercado;

- Disponibilização fluxos de caixa distintos para as operações com ou sem garantia;

- Permitir a remoção de qualquer produto do fluxo de caixa e a inclusão do mesmo no saldo inicial, com algum deságio, considerando prazos de liquidação específicos;

- Permitir uso de alarmes quando limites pré-estabelecidos de saldos forem superados;

- Permitir a avaliação dos cenários em dias, semanas, meses e anos; Permitir a realização de simulações sem alterar os fluxos originais;

- Permitir a entrada de dados para hipóteses de TR, IGP´S, TJLP, US$ e CDI visando a simulação dos fluxos de caixa;

- Permitir a inclusão de valores nos fluxos de caixa simulados; Permitir a eliminação de quaisquer fluxos de caixa eleitos nos fluxos de caixa simulados;

- Permitir a alteração dos valores de resgates de passivos nos fluxos de caixa simulados.

4- Existem relatórios que permitam o monitoramento dos riscos de liquidez assumidos emitidos para a Alta Administração?

5- São feitas avaliações voltadas à identificação de mecanismos e instrumentos que permitam a obtenção dos recursos necessários para reversão de posições que coloquem em risco a situação econômico-financeira da instituição, englobando as alternativas de liquidez disponíveis nos mercados financeiros e de capitais?

6- São realizados periodicamente testes de avaliação dos sistemas de controle implantados, incluindo testes de estresse, testes de aderência e quaisquer outros que permitam a identificação de problemas que, de alguma forma, possam comprometer o equilíbrio econômico-financeiro da instituição;

7- É estabelecido um plano de contingência contendo estratégias de administração de situações de crise de liquidez?

8- O Plano de contingência engloba os seguintes fatores:

- Descrição das obrigações detalhadas do pessoal chave numa situação de crise;
- Definição e quantificação periódica das fontes de recursos vulneráveis e não vulneráveis, bem como dos ativos líquidos;
- Definição da volatilidade de mercado necessária para o equivalente encurtamento dos ativos e redução de operações de crédito;
- Fontes de recursos que provavelmente continuarão com a instituição em qualquer circunstância e se tais recursos podem ser incrementados;
- Fontes de recursos que deverão se retrair gradualmente caso surjam problemas;
- Preço dos depósitos necessários para controlar a velocidade dos saques;
- Tipos de passivos com vencimentos não-contratuais que espera-se que sejam sacados de imediato;
- Montante dos passivos cujo saque antecipado é provável;
- Linhas de reserva que a instituição pode sacar e em que circunstâncias.

**Risco de Modelagem**

1. Os modelos foram formalmente aprovados pela Alta Administração?
2. A Alta Administração conhece as alternativas e as decisões e se foram tomadas com base na relação custo-benefícios, além dos objetivos estratégicos da instituição?
3. Todos os parâmetros e variáveis foram incluídos no modelo?
4. Todas as premissas sobre as variáveis foram avaliadas?
5. Foram realizados testes estatísticos para verificar se as hipóteses feitas sobre as variáveis podem ser rejeitadas com base nos resultados passados?
6. Os resultados obtidos estão em conformidade com os observados no mercado?
7. O modelo prevê de forma precisa os resultados do problema modelado?
8. O modelo trata adequadamente a questão de não linearidade existente em determinados instrumentos financeiros com cláusula de opcionalidade?
9. Quando aplicável, o modelo mapeia adequadamente os fatores de risco nos instrumentos financeiros?
10. O modelo mapeia adequadamente a estrutura a termo de taxas de juros nacionais e internacionais, de forma que as simplificações não alterem o resultado do modelo?
11. As fórmulas de cálculo das planilhas ou dos logaritmos nos sistemas são feitas de acordo com as premissas estabelecidas pela Alta Administração?
12. Quais são os critérios utilizados para o cálculo do stress-test?
13. Os referidos critérios assumem premissas extremamente subjetivas ou os cenários são relativamente viáveis num contexto histórico?
14. O stress-test considera como cenário o risco da não variação dos mercados, uma vez que este cenário pode ser extremamente desfavorável para carteiras com estratégias de opções (strangles e butterflies)?

15. O stress-test é feito com cenários de deslocamentos não paralelos na estrutura a termo da taxa de juros (nível, inclinação e curvatura)?
16. Quais são os testes retroativos aplicados aos modelos?
17. Além do teste de Kupiec, é aplicado outros testes, tal como o teste proposto por Christoffersen?
18. Os testes retroativos são feitos com base em resultados hipotéticos e reais?
19. O apreçamento dos ativos é feito em conformidade com a legislação existente?
20. Os modelos utilizam condições de não arbitragem?
21. Os dados são coletados de forma independente?

**Risco de Informação para Tomada de Decisão**

1. São emitidos relatórios que cubram as sete categorias de informações propostas por Moreira?

**Risco de Crédito**

1- Existe uma metodologia para avaliação do risco de crédito, incluindo a geração de um rating por cliente/operação?

2- O risco de crédito é aprovado pela Alta Administração antes da realização das operações e com base no rating do cliente/operação?

3- Todos os produtos que incorrem em risco de crédito são devidamente considerados, especialmente para as operações de balcão?

4- O risco de crédito segue uma política com estratégias e metas definidas pela Alta Administração?

5- Para a gestão do risco de crédito é considerado, além do valor referencial dos contratos e os prazos, o risco de crédito "potencial" que estima, entre outros, os indexadores da operação?

**Risco Legal**

1- O qual confiável são os controles sobre a identificação das alterações regulamentares, incluindo a forma e freqüência de identificação dos normativos emitidos pelos órgãos reguladores?

2- Como a responsabilidade pelo atendimento a essas novas regulamentações é delegada aos funcionários, ou seja, como é definido quem são os responsáveis por fazer o que?

3- Como é monitorada a conformidade em relação à prestação de informações aos órgãos reguladores, ou seja, como os gestores se asseguram que as diversas informações solicitadas pelos órgãos reguladores, especialmente o Banco Central do Brasil e a CVM, são repassadas de forma tempestiva, completa e íntegra?

4- Qual o nível de aprovação formal, incluindo a verificação independente por pessoa com alçada antes do envio das informações?

5- Os livros societários estão atualizados e devidamente constituídos?

6- A base de cálculo dos tributos é devidamente revisada, atentando para a conformidade com a legislação?

7- As operações classificadas como hedge são devidamente classificadas em conformidade com a legislação?

8- Existe identificação documental do risco objeto de hedge, com informação detalhada sobre a operação, destacados o processo de gerenciamento de risco e a metodologia utilizada na avaliação da efetividade do hedge desde a concepção da operação?

9- É previsto a necessidade de renovação ou de contratação de nova operação no caso daquelas em que o instrumento financeiro derivativo apresente vencimento anterior ao do item objeto de hedge?

10- A efetividade do hedge é devidamente comprovada dentro dos limites estabelecidos na legislação?
11- Existem políticas que definam de forma clara os documentos necessários para realização de cada tipo de operação?
12- Existe aprovação formal do Departamento Jurídico de todos os contratos antes da assinatura dos contratos;
13- É feita a avaliação dos controles sobre a verificação formal dos poderes de alçada das contrapartes com o objetivo de garantir que os contratos estejam bem representados;
14- É feita a avaliação da legitimidade da instituição praticar determinados atos previstos em lei e no seu estatuto social;

**Outros Riscos**

1- Existe um Código de Conduta na instituição, com a inclusão de um Termo de Adesão assinado por todos os funcionários?
2- Existem regras quanto a negociação com entidades/subsidiárias da instituição ou com membros da alta administração?
3- Existem regras quanto a negociação com outros funcionários da instituição?
4- Existem regras quanto aos negócios pessoais dos operadores nos mercados financeiros?
5- Existem regras quanto a relacionamento pessoal com os corretores com os quais o banco opera?
6- Existem regras quanto a escolha das corretoras, alçadas de aprovação e volume de operações por corretora?
7- Existem regras quanto a negociações fora do expediente ou fora das instalações do banco?
8- Existem regras quanto a utilização de telefones celulares?
9- Existem regras quanto a política de remuneração variável? Esta regra não transmite sinais extremamente conflitantes de risco x retorno aos operadores?
10- As atividades de de aprovação de limites, registro, monitoramento e liquidação das transações da tesouraria, são segregadas e gerenciadas de forma independente da mesa de operações?
11- A estrutura organizacional permite a independência entre as atividades do back-office, middle-office e front-office?
12- As boletas de registro possuem as seguintes informações: Identificação por número seqüencial, data e hora; Responsáveis pela aprovação, efetivação e

conferência; Contrapartes; Instrumento, preço, montante e prazo; Despesas de corretagens e comissões e valores de margens?

13- São realizados processos de conferência independente, com a formalização das aprovações de, pelos menos, os seguintes relatórios: Registro gerencial dos operadores com o sistema operacional; Sistema operacional com o sistema contábil; Sistema contábil com as câmaras de compensação (CBLC, BM&F, Selic, Cetip, etc..) Sistema operacional com os relatórios das corretoras; Sistema operacional com os sistemas de gerenciamento de riscos; Performance dos operadores com a conta de lucros e perdas gerenciais e sistema contábil com os relatórios de envio aos órgãos reguladores?

**REFERÊNCIAS BIBLIOGRÁFICAS**


AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS. (1958) Statement on Auditing Standard (SAS) no. 29. New York. USA. 1958.

_____. (1988). Statement on Auditing Standard (SAS) no. 55. New York. USA. 1988.

_____. (1992). Statement on Auditing Standard (SAS) no. 70. New York. USA. 1992.

ANDRADE, A.. (1999) Eficácia, eficiência e economicidade: como atingi-las através dos controles internos. São Paulo. Brasil. 1999.

ANTUNES, J.. (1998). Contribuição ao estudo de risco e controles internos na auditoria das demonstrações contábeis no Brasil. Dissertação (Mestrado em Contabilidade). Faculdade de Economia, Administração e Contabilidade. Universidade de São Paulo. 1998.

ARCOVERDE, G.L. (1999) Alocação de capital para cobertura do risco de mestrado da taxas de juros de natureza pré-fixada. Dissertação (Mestrado em Economia). Fundação Getúlio Vargas. Rio de Janeiro. Brasil. 1999.

BANCO CENTRAL DO BRASIL. Resolução 2554. Brasilia: Bacen. 1998.

_____. Resolução 2804. Brasilia: Bacen. 1998.

_____. Resolução 3086. Brasilia: Bacen. 2002.

_____. Resolução 3096. Brasilia: Bacen. 2002.

_____. Manual da Supervisão. Relatório Técnico. Brasilia: Bacen. 2002.

BANGIA, A., (1998) Modelling liquidity risk, with implications for tradicional market risk measurement and management. University of Pennsylvania, The Wharton Financial Institucions Center, Documento de Trabalho, Dezembro de 1998.

BARBOSA, D. O ; SPECCHIO, S. R. A.; PUGLIESI, W. R.. Novas Metodologias. IBCB, 1999, São Paulo.

BASLE COMMITTEE ON BANKING SUPERVISION. (1998). "Estrutura para avaliação do sistema de controles internos". Basiléia. Suíça. Bank for International Settlements. 1998.

_____. (1994). Amendment to the Capital Accord to Incorporate Market Risk, Suíça. Basileia: Bank for International Settlements. 1994

_____. (1996). Supervisory Framework for the use of "backtesting" in conjunction with the internal model approach to market risk capital requirements. Basiléia, Suíça. Bank for International Settlements. 1996

_____. (1997). Core Principles for Effective Banking Supervision. Basiléia, Suíça. Basiléia. Bank for International Settlements. 1997.

_____. (1998). Framework for internal controls in banking organizations. Basiléia, Suíça. Bank for International Settlements. Setembro. 1998

_____. (2001). The New Basiléia Capital Accord. Basiléia. Suíça. Bank for International Settlements. 2001.

_____. (2003). Overview of The New Basiléia Capital Accord. Basiléia. Suíça. Bank for International Settlements. 2003.

CAMPBELL, S. D. (2005) A Review of BackTesting and BackTesting Procedures. Finance and Economics Discussions Series. Division of Research & Statistics and Monetary Affairs. Federal Reserve Board, Washington D.C. 2005.

CARVALHO, J. E. (2003). Gerenciamento do Risco Operacional em organizações financeiras de 2003. In: Duarte , A.M.; VARGA G. (Org). Gestão de Riscos no Brasil. Rio de Janeiro: Financial Consultoria, 2003. Cap.27.

CHRISTOFFERSEN, P. (1998) "Evaluating interval forecasts", International Economic Review; 39:841-42). 1998.

COELHO, V. A.; MACAHYBA, L. e BERTOLOSSI, F. M.. (2003). Precificação de títulos públicos: metodologia e evidências sobre padrões de comportamento no tempo. In: Duarte, A. M.; Varga G. (Org). Gestão de Riscos no Brasil. Rio de Janeiro: Financial Consultoria, 2003. Cap.12.

COMMITTEE OF SPONSORING ORGANIZATION. (1994). Internal Control: Integrated Framework, Executive Summary, USA, 1994.

CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (1998). CobiT Audit Guidelines. Information System Audit and Control Association. 1998.

CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO.(1998). Controle Interno das Empresas. Ed. Atlas. São Paulo, 1998.

CONSELHO DE RECURSOS DO SISTEMA FINANCEIRO NACIONAL. Recurso 430. Processo BCB0001029787. 235ª Sessão em 24 de março de 2004. Ata publicada no Diário Oficial da União de 24/05/2004.

CORREIA, A. C.. (2001). Lições de falências do Barings- British Bankers´Association. Brasilia. 2001.

CRUZ, G.M. (2003). Modelagem quantitativa do risco operacional. In: Duarte, A. M.; Varga G. (Org). Gestão de Riscos no Brasil. Rio de Janeiro: Financial Consultoria, 2003. Cap.29.

_____. (2002). Modelling, Measuring and Hedging Operational Risk. London: Wiley,2002.

D´AVILA, M. Z. & Oliveira, A.M. . (2002). Conceitos e Técnicas de Controles Internos de Organizações. São Paulo: Nobel, p.15-17, 2002.

DUARTE, A. M. e LELIS, R. J. F.. (2002). Alocação de Capital em Bancos no Brasil. Serasa. Julho 2002.

DUARTE , A. M.. (1997) Model Risk and Management. Derivatives Quartely. Institutional Investor, Inc. n.3, vol.3, Primavera, 1997.

_____. (1999) A Importância do Gerenciamento de Riscos Corporativos. Resenha BM&F. São Paulo: Bolsa de Mercadorias & Futuros, n.133, jul./ago. 1999.

_____. (2005). Gestão de Riscos para Fundos de Investimentos. São Paulo. Practice Hall, 2005.

FEBRABAN (2005a); Pesquisa sobre práticas de gestão de riscos operacionais no mercado brasileiro. Federação Brasileira de Bancos – FEBRABAN, Pricewaterhouse Coopers; São Paulo: IBCB,2005.

_____. (2005b) Auditoria em tesouraria. Federação Brasileira de Bancos – FEBRABAN, Pricewaterhouse Coopers; São Paulo: IBCB,2005.

GRUPO DE TRABALHO ABBI/FEBRABAN (2004). Documento Consultivo – Função de Compliance. Disponível em www.febraban.org.br. Acesso em 21 fev. 2006.

INSTITUTE OF INTERNAL AUDITORS. (1994). System Auditability and Control Report. [1994]

JORION. P. (1997). Value At Risk. MacGrawHill, New York,1997.

KUPIEC, P. (1995), "Techniques for Verifying the Accuracy of Risk Managements Models," Journal of Derivatives, 3, 1995, 73-83.

LONGO, E. C. F.. (2005). Uma breve visão do gerenciamento do Risco de Mercado e Cálculo do VaR. Andima. 2005.

MARSHALL, C. (2002). Medindo e gerenciando riscos operacionais em instituições financeiras. Rio de Janeiro: Qualitymark. 2002.

MAGLIAVACCA, P. N. (2002). Controles internos nas organizações. São Paulo: Edicta, 2002.

MOREIRA, R. L.. (2002). A administração da tesouraria sob o Novo Acordo de Capital da Basiléia. 2002. Dissertação (Mestrado em Administração) – Faculdades Ibmec, Rio de Janeiro, Brasil.

_____ (2003). Transparência e Basiléia II. 2003. In: Duarte, A. M.; Varga G. (Org). Gestão de Riscos no Brasil. Rio de Janeiro: Financial Consultoria, 2003. Cap.5.

NETO, B.C.; GALHARDO, L. C. e CRESTO, V. (2002). Importância da auditoria na avaliação dos controles internos da empresa. Resenha BM&F, 162. 2002

NETO, C. A. V. e URBAN, F..(2003) Um modelo de estresse menos subjetivo e mais abrangente. In: Duarte, A. M.; Varga G. (Org). Gestão de Riscos no Brasil. Rio de Janeiro: Financial Consultoria, 2003. Cap.11.

O´HARA, M. (1995). Market microstructure theory. Massachusetts: Blackwell Publishers.

PERSON, N. e LINSMEIER, T.. (1994). Risk Management: An introduction to Value at Risk. University of Illinois at Urbana-Champaign. Julho. 1994.

PricewaterhouseCoopers (2005). Banana Skins 2005. The CSFI´s annual survey of the risks facing banks. Centre for the Study of Finnancial Innovation. [2005]

SANTOS, S. (2004). Risco legal no mercado de derivativos: a regulamentação à luz da norma contábil. Resenha BM&F, 165. 2004.

SECURATO, J. R.. (1999) “Cálculo Financeiro das Tesourarias”: São Paulo: Saint Paul Institute of Finance. 1999.

SECRETARIA DA RECEITA FEDERAL (2002). Instrução Normativa 247. Artigo 27. 2002.

VALOR ECONÔMICO. Empresa do BankBoston é autuada. Matéria publicada em 11/03/05.

VALOR ECONÔMICO. CVM aplica pena máxima e multa BofA em R$ 2 milhões. Matéria publicada em 15/10/04.

VICENTE, L. A. B. G.. (2003) In: Duarte, A. M.; Varga G. (Org).. Risco de Liquidez – aspectos conceituais e alternativas para sua modelagem. Gestão de Riscos no Brasil. Rio de Janeiro: Financial Consultoria, 2003. Cap.16.

# Livros Grátis

( http://www.livrosgratis.com.br )

Milhares de Livros para Download:


Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo