
Governança Corporativa Gestão de Riscos

Introdução

As constantes mudanças no âmbito global têm fomentado a necessidade do aprimoramento dos controles executados pelas organizações e do ambiente de riscos, resultando em alterações nas diretrizes de gestão dos riscos para a tomada de decisão.

Para mitigar os riscos do mundo corporativo, os órgãos reguladores utilizaram-se da publicação de normas, garantindo a padronização das metodologias utilizadas para a gestão eficiente de seus riscos por parte das instituições financeiras.

Esta gestão eficiente dos riscos está inserida nas boas práticas de governança corporativa. Conforme definição do Instituto Brasileiro de Governança Corporativa (IBGC), a governança corporativa é o "sistema que assegura aos sócios-proprietários o governo estratégico da empresa e a efetiva monitoração da diretoria executiva. A relação entre propriedade e gestão se dá através do conselho de administração, a auditoria independente e o conselho fiscal, instrumentos fundamentais para o exercício do controle. A boa governança corporativa garante equidade aos sócios, transparência e responsabilidade pelos resultados".

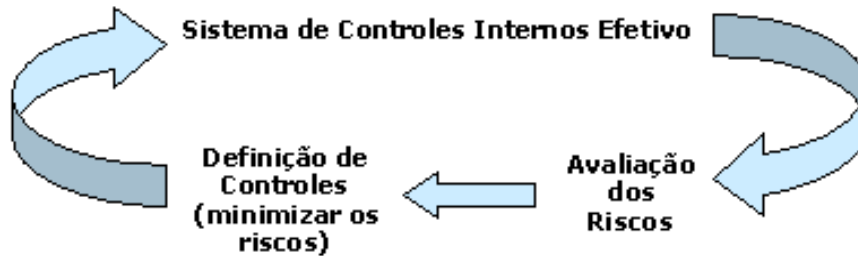
Ou seja, a Governança Corporativa é o conjunto de processos, costumes, políticas, leis, regulamentos e instituições que regulam a maneira como as empresas são administradas e, principalmente, a garantia de que todos os agentes estão em conformidade com os princípios da organização, atuando de forma ética.

Gerenciamento de Riscos

O gerenciamento de riscos nas organizações visa a redução dos impactos dos riscos, caso eles venham a se materializar. Este gerenciamento vai além da avaliação de suas probabilidades de perda, abordando também o estabelecimento de medidas que visem a mitigação dos riscos ao longo do tempo.

Para gerenciar os riscos, são estabelecidos controles que minimizam seus impactos, aprimorando o sistema de controles internos da instituição. Este gerenciamento concentra-se na busca de oportunidades, obtendo vantagem competitiva e aumento do valor para o acionista.

Estratégias/Objetivos



FONTE: Banco ibi

A Administração do Banco ibi e suas áreas de Compliance e a Auditoria trabalham em conjunto para garantir a governança corporativa e a eficiência dos Controles Internos da organização, sendo que cada uma delas apresenta responsabilidades específicas: (i) a Administração deve exercer sua responsabilidade ao buscar uma forma de gerenciar o risco do negócio, proporcionando segurança operacional e maior credibilidade aos seus stakeholders; (2) Compliance deve assegurar o fortalecimento e o funcionamento do modelo de Controles Internos, mitigando os riscos e disseminando a cultura de controles e o cumprimento da legislação em conjunto às áreas de negócios e (3) a Auditoria responsabiliza-se por verificar a conformidade dos controles existentes.

O Banco ibi se baseia na metodologia definida pelo COSO (Committee of Sponsoring Organizations), entidade sem fins lucrativos, que visa a melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e da governança corporativa, para gestão de riscos e controles internos.

Entende-se por controles internos todas as políticas, procedimentos e práticas instituídas para assegurar que os riscos inerentes às atividades da instituição sejam identificados e gerenciados. O objetivo principal dos controles internos é auxiliar a entidade a atingir seus objetivos, lembrando que o controle interno é um elemento que compõe o processo de gestão. A estrutura do sistema de controles do COSO divide-se em elementos que estão inter-relacionados e presentes em todo controle interno, conforme figura abaixo:

Sistema de Estrutura Integrada (COSO)



FONTE: COSO (Committee of Sponsoring Organization)

(1) Ambiente interno – cultura de controle que envolve a competência técnica e o compromisso ético das pessoas, englobando fatores como integridade, formas de consulta, políticas de recursos humanos, estrutura da organização e a responsabilidade da Alta Administração com a cultura de controles. Através do Código de Ética, o ibi reforça seus valores e principais políticas, contando com a independência das áreas de Compliance e Auditoria Interna e da utilização de intermediadores e facilitadores de Compliance na figura dos Business Unit Compliance Officer (BUCOs);

(2) Fixação de objetivos – estabelecimento dos objetivos estratégicos e como atingi-los, visando assegurar o alinhamento entre os objetivos e a visão com o apetite e a tolerância ao risco. No Banco ibi, os riscos são avaliados pela Alta Administração e as diretrizes da instituição são compartilhadas com os gestores das áreas;

(3) Identificação de eventos – identificação de riscos com o objetivo de mapear os eventos de riscos que possam afetar as estratégias da instituição. A identificação de eventos no Banco ibi ocorre através da realização do self-assessment com o envolvimento dos responsáveis pelos processos e da Alta Administração;

(4) Avaliação dos riscos – identificação e análise dos riscos associados à operação sob as perspectivas quantitativa e qualitativa. No enfoque quantitativo são utilizados modelos para avaliação das eventuais perdas esperadas e inesperadas e a base de perdas históricas, enquanto no enfoque qualitativo os riscos são avaliados com base na severidade e na probabilidade para indicar o grau de exposição ao risco. O ibi realiza a avaliação dos riscos através do manuseio de sua base de perdas e do resultado obtido com o self-assessment realizado pelas áreas;

(5) Resposta a risco – identificação e avaliação das opções de resposta ao risco, considerando seus efeitos na probabilidade e no impacto do evento, com relação à tolerância ao risco e à relação custo/benefício. A resposta ao risco, no Banco ibi, é analisada em conjunto com os responsáveis das respectivas áreas, visando à definição do tratamento adequado dos riscos;

(6) Atividades de controle – atividades que, quando executadas a tempo e de maneira adequada, permitem a redução ou administração dos riscos. São elas: alçadas, autorizações, conciliação, revisões de desempenho, segurança física, segregação de funções, sistemas informatizados e normatização interna. O ibi apresenta um Sistema de Controles Internos descentralizado sob responsabilidade dos gestores das áreas, que realizam a identificação, avaliação, revisão e o mapeamento de seus riscos;

(7) Informações e comunicações – fluxo de informações dentro da organização. Quanto à informação e comunicação, o ibi disponibiliza um canal de denúncias (Canal Aberto) entre seus funcionários, além de disponibilizar na intranet todos os normativos pertinentes à operação da instituição, disponíveis a todos os funcionários. Também são elaborados relatórios de Auditoria que permitem à Alta Administração monitorar o ambiente de controles e as ações corretivas adotadas pelas áreas;

(8) Monitoramento – avaliação dos controles internos ao longo do tempo através do acompanhamento contínuo das atividades para verificar se estes são adequados e efetivos. No ibi, as auditorias interna e externa realizam o monitoramento da gestão de riscos e reportam, quando necessário, os casos de não-conformidade à Alta Administração e ao Comitê de Risco Operacional.

Risco Operacional

Segundo definição do Banco Central, através da publicação da Resolução 3.380 em jun/2006, risco operacional é a “possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos, incluindo o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanções em razão de descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição”.

Baseada nesta definição, o banco ibi adota como definição de risco operacional “o risco de perda resultante de processos internos, pessoas e sistemas inadequados ou falhos, ou de eventos externos”.

O Risco Operacional divide-se nos seguintes eventos:

- Fraude Interna: Comportamentos fraudulentos e/ou criminosos com intenção de obter ganhos pessoais e/ou subtrair a propriedade alheia em benefício da instituição.
- Fraude Externa: Pessoas que não pertencem à instituição exercerem atividades irregulares em benefício próprio.
- Relações Trabalhistas: Decisões judiciais por práticas incompatíveis com leis/acordos trabalhistas, nocivas à saúde/segurança dos funcionários ou por discriminação/diferenciação no tratamento.
- Falhas de Sistemas: Impossibilidade de obter informações devido à falha de comunicação, perda da capacidade de processamento ou dificuldade na operação dos sistemas.
- Execução e Gestão de Processos: Disponibilidade, Registro de informações inválidas, incompletas ou de maneira intempestiva a entidades externas, órgãos reguladores, acionistas e investidores.
- Práticas Comerciais: Falta de cumprimento de padrões éticos e comportamentais estabelecidos e práticas inadequadas do pessoal de vendas. Orientação/Consultoria inadequada a clientes que leve a falsas expectativas quanto à rentabilidade/custo das operações.
- Danos a Ativos: Desastres naturais e outros eventos que ocasionem perdas físicas a ativos da companhia.

- Interrupção das atividades: Impossibilidade de sustentar as operações, prover serviços essenciais ou recuperar custos operacionais decorrentes de desastres controláveis ou não.

Modelo de Gestão de Risco Operacional

Para a adequada gestão de risco operacional, o Banco ibi conta com a sinergia entre as áreas de Compliance, Auditoria Interna, Processos e Qualidade, Segurança da Informação, Controladoria, entre outras, ressaltando que todas as definições são analisadas pela Alta Administração.



FONTE: Banco ibi

No ibi, a identificação do risco operacional ocorre em dois momentos: quanto às informações qualitativas, ocorre através do self-assessment e quanto às informações quantitativas, ocorre através da base de perdas.

No self-assessment, o ibi adota o conceito de risco inerente e risco residual. Entende-se por risco inerente a avaliação dos riscos sem considerar a execução de controles para mitigá-lo, enquanto o risco residual compreende a avaliação dos riscos após a consideração dos controles. Esses conceitos permitem que os controles sejam avaliados e que sua efetividade seja comprovada durante os testes das auditorias.

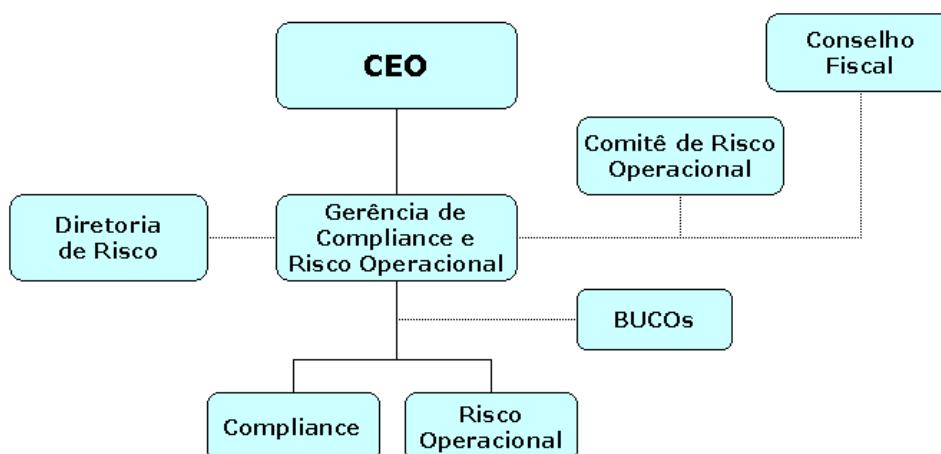
A avaliação dos riscos é realizada pela Alta Administração e acompanhada periodicamente.

O monitoramento das correções e reporte ocorre através das atividades das auditorias, cujo reporte é feito à Alta Administração e, por fim, o processo estruturado de comunicação ocorre através do acompanhamento das perdas, avaliação e monitoramento pelo Comitê de Risco Operacional, além da utilização de canais de comunicação internos.

Estrutura de Gestão do Risco Operacional

Com objetivo de adequar-se a Resolução 3.380 do Banco Central, o Banco ibi estruturou a gestão do risco operacional dentro da Gerência de Compliance.

Organograma da Estrutura do Risco Operacional



FONTE: Banco ibi

A Gerência de Compliance e Risco Operacional preserva sua independência através do reporte direto ao CEO da organização, contando com o reporte matricial para a Diretoria de Risco, sendo esta a diretoria indicada pela Alta Administração, junto ao Banco Central, como responsável pelo Modelo de Gestão de Riscos Operacionais.

O Comitê de Risco Operacional é composto pelas áreas de Controladoria, MIS, Processos e Qualidade, Compliance e Risco Operacional e Alta Administração.

O ibi como melhores práticas em governança corporativa instituiu o Conselho Fiscal, atuando ativamente na avaliação dos controles internos, compliance e gestão de riscos.

Método de Alocação de Capital

Com a divulgação do Acordo da Basileia revisado, conhecido como Basileia II, introduziu-se o requerimento de alocação de capital para o risco operacional. O novo acordo baseia-se em três pilares:



FONTE: Base Committee on Banking Supervision

Para alocação de capital (Pilar I), os métodos existentes são:

- Método Básico (BIA) : não há diferenciação entre as linhas de negócio. Utilização de um fator único para apuração da alocação de capital;
- Método Padronizado (STA): segregação do resultado por linhas de negócio. Utilização de fatores diferenciados para a apuração da alocação de capital;
- Método Padronizado Alternativo (ASA): segregação do resultado por linhas de negócio e tratamento diferenciado para as linhas "comercial" e "varejo". Utilização de fatores diferenciados para a apuração da alocação de capital;
- Método Avançado (AMA): critérios qualitativos e quantitativos internos para a apuração da alocação de capital.

Conforme cronograma divulgado pelo Banco Central em alinhamento com as normas internacionais, o Banco ibi adotou, em junho de 2008, o método básico como metodologia para a apuração da alocação de capital. A instituição vem realizando um trabalho contínuo de alinhamento às melhores práticas de mercado na gestão de risco operacional.