BANCO DE INVESTIMENTOS CREDIT SUISSE (BRASIL) S.A.
R. Leopoldo Couto de Magalhães Jr., 700 Tel: (11) 3701.6000
10º andar - São Paulo - SP 04542-000 Fax: (11) 3701.6900

Risco Operacional

1. Definições básicas

As instituições financeiras e as demais instituições autorizadas a funcionar pelo Banco Central do Brasil devem implementar e manter uma estrutura de gerenciamento integrado, em conformidade com os termos da Resolução 4.557 de 23 de fevereiro de 2017, compatível com o modelo de negócio, com a natureza das operações e a com a complexidade dos produtos, serviços, atividades, processos e sistemas da instituição.

O risco operacional é definido como a possibilidade de ocorrência de perdas ou ganhos resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas e sistemas. Essa definição inclui o risco legal, que é o risco de perdas resultantes de falhas no cumprimento de leis/regulamentações e obrigações contratuais (legal risk). Também inclui a exposição à litígios derivados das atividades do CS. Essa definição exclui riscos estratégicos e reputacionais. No entanto, é sabido que alguns riscos operacionais podem levar a questões reputacionais.

A estrutura de gerenciamento do risco operacional visa principalmente identificar, avaliar, monitorar, reportar, controlar e mitigar os riscos inerentes associados ao CS Brasil, além de documentar informações referentes às perdas/ganhos associadas ao risco operacional.

2. Estrutura básica

O CS Brasil adota estrutura de gerenciamento contínuo do risco operacional, nos termos exigidos pela Resolução 4.557 do Banco Central do Brasil de 22 de fevereiro de 2017. A gestão do risco operacional e de conformidade é de responsabilidade de todos os funcionários do CS. Os gestores com a ajuda das áreas de primeira linha de defesa são responsáveis pela identificação, classificação, gestão e reporte dos riscos inerentes ao desenvolvimento de suas atividades. Também inclui a definição, operacionalização e garantir a performance e efetividade dos controles que são requeridos para aderência ao apetite de risco e políticas internas. As áreas de segunda linha de defesa são responsáveis por estabelecer a estrutura para a gestão do risco operacional e padrão dos controles associados e prover avaliação e desafio – de forma independente – em relação às atividades processos e controles implementados e executados pela primeira linha de defesa. Ainda, a terceira linha de defesa é responsável por avaliar de forma independente para a diretoria/alta administração e Comitê de Auditoria a adequação da estrutura de gestão de riscos e controles e criar mecanismos de avaliação dos processos relativos à gestão de riscos e controles da primeira e segunda linhas de defesa.
Como suporte ao processo de monitoramento independente do risco operacional, o CRO (Chief Risk Officer) conta com a estrutura da área de ORM/NFR (Operational Risk/Non-Financial Risk). A área de ORM/NFR, entre outras atividades, é responsável por monitorar de forma contínua e consolidada as perdas/ganhos operacionais em relação ao apetite de risco definido para as entidades do conglomerado Brasil e reportar os níveis de utilização, bem como eventuais excessos ao Comitê de Gerenciamento de Riscos e Capital (CRMC).

A divulgação e a disseminação da cultura de riscos e controles e a tomada de risco disciplinado e transparente são de responsabilidade de cada área. O CS disponibiliza aos funcionários, através da sua intranet, treinamento mandatório das políticas relacionadas à esturura de riscos e controles.

3. Responsabilidades

3.1. Gestores/Supervisores

São responsáveis por:

- Identificar, acessar e gerenciar continuamente os principais riscos operacionais e de conformidade da sua área de responsabilidade;
- Supervisionar os funcionários adequadamente;
- Comunicar incidentes de risco operacional material, quando ocorrerem, e tomar as ações necessárias para mitigar/escalar apropriadamente;
- Estar familiarizado e garantir a aderência dos padrões de Conduta e Ética do CS;
- Avaliar regularmente a eficácia do gerenciamento dos principais riscos operacionais em suas áreas de responsabilidade;
- Manter estrutura de controles adequada para mitigar o risco operacional;
- Garantir que sejam registrados no sistema global de risco operacional do CS todo incidente de risco operacional (ganhos e perdas), relacionados à sua área de responsabilidade, de acordo com os critérios, prazos e limites estabelecidos em políticas/procedimentos internas;
- Reportar, escalar, gerenciar, analisar e remediar incidentes internos de acordo com os critérios, prazos e limites estabelecidos em políticas/procedimentos internos;
- Escalar tempestivamente à diretoria executiva e ao Comitê de Gerenciamento de Riscos e Capital, quando ocorrerem incidentes de risco operacional relevantes ou quando os níveis de exposição ao risco excederem os limites definidos na RAF/RAS e nas políticas/procedimentos internos aplicáveis;
- Conduzir avaliação de causa raiz de incidentes internos relevantes e definir, implementar e monitorar ações mitigatórias, quando aplicável, conforme estabelecido em políticas/procedimentos interno

3.2. Todos os Funcionários (Colaboradores atuando nas áreas de negócio/ Primeira linha de defesa/Funções Corporativas)

São responsáveis por:

- Dar ciência e gerenciar os riscos operacionais e de conformidade relacionados às funções que desempenha e ao seu ambiente de trabalho;
- Escalar à supervisão preocupações relacionadas ao ambiente de riscos operacionais e de conformidade;
- Reportar aos gestores, registrar e garantir que sejam registrados no sistema global de risco operacional do CS todo incidente de risco operacional (ganhos e perdas),

relacionados à sua área de responsabilidade, de acordo com os critérios, prazos e limites estabelecidos em políticas/procedimentos internos;

- Reportar, escalar, gerenciar, analisar e remediar incidentes internos conforme estabelecido em políticas/procedimentos internos;
- Conduzir avaliação de causa raiz de incidentes internos materiais ou que excedam os limites definidos na RAF/RAS e nas políticas/procedimentos internos e definir, reportar e monitorar a implementação de ações mitigatórias, quando aplicável, em colaboração com o time de ORM/NFR.

3.3. ORM/NFRM

A área de ORM`/NFR é responsável por supervisionar e avaliar de forma independente a implementação e efetividade da estrutura de gestão dos riscos não-financeiros das divisões e funções corporativas do conglomerado Brazil, em parceria com as áreas globais de Non-Financial Risk de cada divisão/função corporativa. Tal supervisão é executada através das seguintes atividades :

- conduzir revisão/análise independente dos resultados da avaliação de riscos e controles que é realizada anualmente por cada Divisão, em relação aos riscos cuja responsabilidade seja atribuída ao grupo de Ops Risk/NFR;
- obter com o Financial Control/Tax, analisar e manter arquivado o relatório mensal de perdas/ganhos decorridos de incidentes operacionais registrados na contabilidade local;
- reconciliar o arquivo de perdas/ganhos registrados na contabilidade local com as informações registradas no sistema de risco operacional do CS de forma a garantir que os incidentes sejam reportados conforme critérios, prazos e limites estabelecidos em políticas/procedimentos internos. Eventuais divergências bem como as ações concordadas para sanar respectivas divergências são reportadas ao COO de cada divisão e ao Comitê de Gerenciamento de Riscos e Capital, onde as ações de correção são também monitoradas;
- prover avaliação independente dos dados registrados no sistema de risco operacional do CS, incluindo qualidade da informação na descrição do incidente e do “lessons learned ”, identificação adequada da causa raiz, classificação da severidade, prazos para registro e aprovações. Garantir que os incidentes internos materiais sejam devidamente avaliados pelas respectivas divisões e reportados para os comitês relacionados;
- instigar as divisões a revisar temas ou tendências que sejam identificados através de avaliação independente ou de repetição de incidentes internos que possam indicar um aumento de exposição ao risco operacional;
- acompanhar a evolução das normas regulamentares relacionadas a risco operacional e cuidar de sua divulgação interna;
- apresentar ao Comitê de Gerenciamento de Riscos e Capital do grupo CS Brasil as métricas de perdas operacionais das entidades do conglomerado, bem como, o nível de utilização da tolerância ao apetite de risco operacional definido para o conglomerado Brasil;
- coordenar a revisão e atualização desse documento, no mínimo anualmente;

- supervisionar a aderência e cumprimento dos requerimentos estabelecidos nas políticas/procedimentos internos e participar da avaliação de incidentes internos materiais ou que excedam os limites definidos na RAF/RAS, quando aplicável, em colaboração com os times de primeira linha de defesa;
- elaborar relatório e resumo com a descrição da estrutura de gerenciamento do risco operacional que deve ser divulgado no sítio do CS Brasil e juntamente com as demonstrações contábeis semestrais, respectivamente.

3.4. Auditoria (Terceira Linha de Defesa)

A Auditoria Interna Local é responsável pela avaliação idenpendente, autonôma e imparcial da qualidade e da efetividade dos sistemas e processos de controles internos exercidas pelos diversos departamentos envolvidos no Gerenciamento do Risco Operacional, como parte do cronograma de auditoria interna, definido de acordo com especificações da Resolução 4.879/2020 e aprovado pelo Comitê de Auditoria local.

3.5. Terceiros

A contratação de terceiros para prestação de serviços às empresas do conglomerado CS Brasil é de responsabilidade do departamento solicitante, cabendo ao gestor do departamento solicitante garantir o cumprimento dos requerimentos relacionados à seleção, avaliação, monitoramento e gestão de risco (incluindo o risco operacional) e performance do referido prestador de serviços, que deve ser feita com base nos padrões mínimos definidos nas políticas internas.
Adicionalmente, cada divisão deverá seguir os requerimentos gerais e específicos definidos na estrutura global.

3.6. Comitê de Gerenciamento de Capital e Riscos

O Comitê de Gerenciamento de Riscos e Capital reúne-se mensalmente para discutir e avaliar a exposição aos riscos, incluindo o risco operacional, revisar os excessos/desvios em relação aos limites estabelecidos e propor, avaliar e acompanhar a implementação de ações corretivas ou de remediacão, caso necessário. São apresentadas no comitê as métricas de perdas/ganhos decorrentes de incidentes operacionais ocorridos no mês anterior, bem como os planos de ação/remediação concordados para mitigar as falhas identificadas, caso o incidente tenha sido considerado material.
Mensalmente, a área de ORM/NFR disponibiliza - via e-mail - aos COOs de todas as divisões e ao COO Brasil o mapa contendo o valor total das perdas financeiras com incidentes operacionais consolidado para o ano. Constam no mapa os valores discriminados por empresa e consolidado para o conglomerado, de todas as despesas lançadas nas contas contábeis de erros operacionais. O mapa também apresenta um destaque dos eventos considerados revelantes.

3.7. Diretoria Executiva

A Diretoria Executiva do CS no Brasil é responsável pela disseminação das políticas, revisão e aprovação anual dos limites estabelecidos na RAS e pelo gerenciamento do risco operacional. E também é responsável por conscientizar os gerentes sobre a importância de manter uma cultura de risco disciplinado e transparente e por garantir a adoção de uma abordagem prudente na tomada de riscos apropriados à estrutura de capital do banco, de forma a preservar seus acionistas e clientes.

4. Base e Coleta de Dados

O CS Brasil possui uma base de dados local, com base em informações extraídas da contabilidade local, para monitorar de forma consolidada as perdas/ganhos decorrentes de incidentes operacionais das entidades do conglomerado.
Adicionalmente, todos os funcionários devem registrar os incidentes operacionais no sistema global de risco operacional do CS, conforme critérios e prazos definidos em políticas/procedimentos internos.
Incidentes que ultrapassem o limite de tolerência individual estabelecido na RAS, devem ser submetidos à uma investigação aprofundada que inclui fatos e cronologia dos eventos, informações detalhadas sobre os processos/controles relacionados ao evento. O processo é liderado pela primeira linha de defesa em parceria com a segunda linha de defesa com participação de outras áreas que sejam consideradas relevantes na avaliação do processo. Os resultados desta avaliação, bem como, os achados e as melhorias recomendadas pela segunda linha de defesa, serão apresentados aos membros do Comitê de Gerencimento de Riscos e Capital.

5. Contabilidade

Os produtos negociados pelo CS Brasil são registrados em sistemas específicos pelas diferentes áreas do banco, de acordo com a natureza de cada um. Esses sistemas alimentam o sistema de Contabilidade (CTB), no qual as operações realizadas podem ser identificadas.
Para documentar e acompanhar os erros operacionais, foram criadas contas específicas no CTB nos grupos de:
a) Despesas administrativas
b) Receitas / despesas operacionais
Os lançamentos dos valores reconhecidos como perdas/ganhos decorrentes de incidentes operacionais são efetuados nas respectivas contas contábeis e podem ser utilizadas por todas as áreas que necessitam registrar erro operacional.
Os analistas da Contabilidade também podem registrar valores como perdas/ganhos decorrentes de eventos operacionais e impactar as contas contábeis mediante solicitação ou identificação dos eventos diretamente pelos gerentes/supervisores e colaboradores das áreas. Isso é feito nos casos de lançamentos de multas com o Banco Central, outras multas e tributos, possíveis despesas com fraudes, assim como outras despesas operacionais de natureza diversas.

6. Estrutura de Contingência

O CS Brasil adota o Plano de Continuidade de Negócios (BCP, na sigla em inglês), o qual prevê a manutenção das atividades consideradas críticas, em caso de contingência. Como parte do Plano, o Banco possui um DR Site (local alternativo para a execução das atividades descritas no BCP), considerado adequado às necessidades atuais da instituição. O atual Plano de Continuidade de Negócios prevê situações em que as estruturas críticas de IT (Information Technology) estariam temporariamente indisponíveis, em que o local de trabalho estaria indisponível devido a algum sinistro e, ainda, situações pandêmicas em que os funcionários não poderiam deixar suas residências.
Ao menos uma vez por ano a equipe interna de IT realiza testes para validar a infraestrutura de IT (sistemas, servidores, bases de dados, links de comunicação, etc.) o teste encaminhando os funcionários para o DR Site, a fim de treiná-los e de validar o BCP do ponto de vista dos negócios.
A atual estrutura de contingência contribui significativamente para o cumprimento da política de gerenciamento de Riscos Operacionais por evitar que possíveis falhas operacionais em IT prejudiquem severamente os negócios. Por isso, a Diretoria Executiva investiu nessa estrutura e emprega uma quantidade adequada de recursos para manter o plano e garantir seu funcionamento.

7. Informação e comunicação

O CS Brasil possui uma intranet local com páginas específicas para cada departamento com informações relevantes disponíveis para todos os funcionários. Além das páginas departamentais, um campo distinto na página inicial oferece informações institucionais importantes, como o Plano de Contingência, o Manual de Controles Internos ("MCI"), link para o portal de políticas globais do CS e políticas de Compliance. Os principais procedimentos internos estão disponíveis no MCI.
A página do Comitê de Auditoria também está disponível a todos na intranet. Nessa página, os funcionários podem relatar, em caráter anônimo ou não, situações que resultaram no descumprimento de dispositivos legais, regulamentos, códigos e normativos aplicáveis à instituição. Trata-se de um canal totalmente independente.
Além disso, todas as políticas globais podem ser acessadas através de intranet Global.

8. Apuração das Perdas/Ganhos e Compensação/Ressarcimento à Clientes

A apuração das perdas/ganhos originados por incidentes de risco operacional deve seguir as diretrizes definidas em políticas/procedimentos internos.
A área de ORM/NFR informa o total das perdas/ganhos ao Comitê de Gerenciamento de Riscos e Capital (CRMC), com destaque para os incidentes com perdas/ganhos relevantes, conforme classificação e limites definidos em políticas/procedimentos internos. Além disso, a área de ORM/NFR reconcilia o arquivo de perdas/ganhos registrados na contabilidade local com as

informações extraídas do sistema global de risco operacional do CS de forma a garantir que as perdas registradas na contabilidade local sejam reportadas conforme critérios, prazos e limites estabelecidos em políticas/procedimentos internos.
As áreas de negócios podem deter procedimentos mais específicos para identificar, analisar, reportar e autorizar o pagamento relativo a ressarcimento/compensação de seus clientes por eventuais perdas originadas de eventos de risco operacional.

9. Estrutura de Governança de IT

O CS Brasil possui estrutura de governança de IT compatível com os níveis de apetite por riscos estabelecidos na RAS (Declaração de Apetite de Risco), bem como, sistemas, processos e infraestrutura de IT que:

- asseguram integridade, segurança e disponibilidade dos dados e dos sistemas de informação utilizados baseando-se em uma plataforma de replicação de dados online para o ambiente de DR Site mantido com um provedor externo. Adicionalmente são utilizados links de dados redundantes para assegurar alta disponibilidade;
- sejam robustos e adequados às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse, através de monitoramento contínuo da infrestrutura (servidores, devices de rede, performance do banco de dados, etc);
- incluam mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir vulnerabilidades e a superfície de ataque, utilizando a plataforma padrão homologada pelo CS;
- Os procedimentos de Governança de IT encontram-se descritos no Manual de Controles Internos;
- *Change & Development Process*, utilizando processos automatizados e ferramentas de controle e registro das mudanças, com as devidas aprovações e segregações de função. O processo de desenvolvimento de sistemas possibilita acompanhamento de todas as etapas, desde a solicitação de uma nova funcionalidade até a entrega final da solução de software;
- Procedimento Local de Suporte e Infraestrutura, com registro detalhado de todos os chamados com classificação de criticidade, alocação dos técnicos e fechamento do chamado. Possibilita ainda levantamento de métricas para acompanhamento. Utilização da ferramenta global para registro de incidentes e de problemas que afetem a plataforma como um todo;
- O processo de governança sobre End User Computing possibilita identificar e controlar eventuais sistemas, ferramentas ou código criados e sob responsabilidade das áreas de negócio e que não possuem a gestão e monitoramento da área de tecnologia da informação.
- Controle de Mudanças e Projetos de IT Infrastucture, com controle de mudanças automatizado com o registro de todas as solicitações e suas respectivas aprovações;

- Política de Acesso a Sistemas e Serviços com controle baseado em perfil das diversas funções exercidas pelos colaboradores, registro de todas as solicitações de acesso com as respectivas aprovações.

10. Avaliação da estrutura de risco operacional

O CS possui uma estrutura de governança global que é responsável por revisar e aprovar periodicamente as ferramentas e metodologias, bem como, alterações nas políticas/ procedimentos e manuais relacionadas à gestão do risco operacional. Adicionalmente, a área de ORM/NFR, em parceria com as áreas globais de NFR de cada divisão e com base em metodologia de avaliação definida no nível global, provê uma avaliação independente da estrutura de gestão do risco não-financeiro das divisões operando no conglomerado Brazil. Os resultados desta avaliação são apresentados aos membros do Comitê de Gerenciamento de Riscos e Capital. A Auditoria Interna avalia, periodicamente, como parte do cronograma de auditorias internas, as atividades de controle exercidas pelos diversos departamentos envolvidos no Gerenciamento de Riscos, incluindo o Operacional.

11. Treinamento

O CS disponibiliza uma agenda periódica de treinamentos que são realizados através de plataformas globais por meio de e-learning a fim de assegurar a adequada disseminação e adequação aos requerimentos das políticas globais, que inclui as políticas de gestão de riscos não-financeiros. Além disso a área de Ops Risk/NFR implementou, a partir de 2020, um treinamento dedicado aos novos funcionários do CS Brasil como uma introdução ao risco operacional, provendo uma visão geral das principais políticas/procedimentos globais da estrutura de gestão do risco não-financeiro aplicáveis ao conglomerado Brazil.