Regulamentações de Compliance Sarbanes-Oxley e Basileia II

Prof. Sergio Nascimento

sergio.onascimento@sp.senac.br

Introdução

Nesta aula vamos estudar, no contexto da Governança de TIC, que as organizações, além do desafio de cumprir suas metas estratégicas de negócio, também, de acordo com sua natureza, devem atender a exigências legais e regulatórias externas.

Por exemplo, empresas do setor de telefonia celular devem atender às exigências da Anatel, os bancos ao Banco Central, as empresas com capital aberto e ações em Bolsa de Valores à Comissão de Valores Mobiliários, as empresas do setor de medicamentos à Anvisa e assim por diante.

A governança corporativa é essencial para o bom atendimento dessas exigências e a Governança de TIC exerce papel fundamental nesse contexto, pelos aspectos operacionais presentes na área de TIC que devem estar em conformidade com as regulações. Para garantir essa conformidade, as empresas utilizam modelos de controles internos e de gestão de risco, sendo o principal deles o **COSO**, com seu módulo "**Internal Control Integrated Framework**", ligado aos controles internos e garantindo-os através das seguintes categorias de objetivos:

- Eficiência e eficácia das operações;
- Confiabilidade das demonstrações financeiras;
- Conformidade com as leis e regulamentos vigentes.

Regulamentações de Conformidade

No ano de 2001 houve uma série de escândalos financeiros em empresas nos Estados Unidos, como os que ocorreram com as empresas Enron e Worldcom, que forjaram uma situação contábil inexistente (lucros maiores que os reais), com a finalidade de gerar bonificações para seus executivos. Isso abalou a confiança dos investidores na Bolsa de Valores, que naquele país é o principal meio de investimento dos recursos das famílias, assim como no Brasil é a caderneta de poupança e a renda fixa. Nesse contexto, essa lei (ato) foi promulgada em agosto de 2002 para aumentar os controles internos sobre os relatórios financeiros das empresas de capital aberto e manter a credibilidade do sistema financeiro, minimizando riscos de fraudes contábeis e financeiras e instituir penalidades na esfera criminal para os responsáveis. A lei levou o nome dos dois congressistas americanos que lideraram os trabalhos.

Nos últimos anos, intensificou-se o foco e a preocupação com o gerenciamento de riscos, e tornou-se cada vez mais clara a necessidade de uma estratégia sólida, capaz de identificar, avaliar e administrar riscos. Em 2001, o "COSO1 " iniciou um projeto com essa finalidade e solicitou à PricewaterhouseCoopers que desenvolvesse uma estratégia de fácil utilização pelas organizações para avaliar e melhorar o próprio gerenciamento de riscos.

A gestão de risco é contemplada pelo módulo do COSO denominado "**Enterprise Risk Management Framework**", que se destina à identificação de riscos operacionais e consequentes controles internos que os atenuem. Nesse contexto, naqueles riscos identificados que envolvem processos de TIC, a área de TIC será a responsável pela implementação dos controles. .

Requisitos da SOX que afetam a TIC

Existem dois regulamentos muito importantes, a **Lei Sarbanes-Oxley (SOX)**, que atinge empresas com ações nas bolsas de valores americanas e também subsidiárias de multinacionais, e o **Acordo da Basileia II (Basileia II)**, que atinge as instituições financeiras. Esses dois regulamentos geram forte impacto na área de TIC.

A implementação e a fiscalização, sob a forma de auditorias periódicas, das regras da SOX, estão sob a responsabilidade da Stock Exchange Commission (SEC), órgão regulador da Bolsa de Valores americana, o equivalente à Comissão de Valores Mobiliários (CVM) no Brasil. Essas regras visam aos relatórios financeiros que são de responsabilidade do CEO (presidente da empresa) e o CFO (diretor financeiro).

Dentro da SEC existe um órgão denominado Public Company Accounting Oversight Board (PCAOB), que é responsável por definir regras e certificar as empresas independentes de auditoria a aplicar os exames de auditorias nas empresas elegíveis.

O CEO e o CFO também são responsáveis pelos controles na emissão dos relatórios financeiros e pelos sistemas de controle interno sobre estes, pelas mudanças que esses controles sofram, suas deficiências e comunicação de fraudes que possam afetar o balanço da empresa.

Implicações da SOX para TIC

Em relação à área de TIC, diversos requisitos a afetam, ligados ao conteúdo da informação, sua disponibilidade sempre que necessário, sua precisão e integridade e que seja acessada pelos funcionários autorizados para tal. Uma vez que os processos de negócio que geram e tratam a informação estão automatizados em sua maioria nas empresas de capital aberto, os requisitos da SOX se aplicam em todos os sistemas transacionais dentro da empresa. A área de TIC, portanto, é um elemento crítico de risco para o atendimento da SOX.

As seções 302 e 404 da Lei da SOX são as aplicáveis no caso da área de TIC. Os principais requisitos da seção 302 se ligam à responsabilidade do CEO e do CFO sobre a revisão, veracidade e precisão das informações dos relatórios financeiros, ou seja, que expressem a real condição financeira da empresa e não apresente omissões ou declarações falsas. A seção 404 trata da responsabilidade da administração da empresa sobre estabelecer e manter os controles internos, sua efetividade e que seja realizada uma auditoria externa que avalie a efetividade do sistema de controles internos da empresa.

Implicações da SOX para TIC – Parte I

Requisitos de qualidade da informação	Implicações do SOX
O conteúdo da informação deve ser apropriado	Processo de desenvolvimento de requisitos de *software* Processo de gerenciamento de requisitos de *software* Métodos de engenharia de *software* Processos de verificação (texto) Processos de validação (solicitação pelos usuários) Processos de segurança da informação empregados nos aplicativos Processos de aceitação de produtos de terceiros Processos de gestão de mudança e de configuração

Implicações da SOX para TIC – Parte II

Requisitos de qualidade da informação	Implicações do SOX
A informação deve estar disponível no momento em que for necessária	Disponibilidade de aplicativos Disponibilidade da infraestrutura Gerenciamento de incidentes e problemas no ambiente de produção Suporte aos usuários Gestão de aplicativos e de ativos de TIC Processos de gerenciamento da infraestrutura Segurança da infraestrutura Gerenciamento de contingência Gerenciamento de disponibilidade e desempenho
A informação é atual ou pelo menos é a última disponível	Processos de gerenciamento de dados Planejamento e gerenciamento da contingência e de desastres Segurança da informação na infraestrutura

Implicações da SOX para TIC – Parte III

Requisitos de qualidade da informação	Implicações do SOX
Os dados e as informações estão corretos	Segurança da informação em aplicativos Segurança da infraestrutura de TIC Teste de *software* Controle da mudança e da configuração Gerenciamento de dados Gerenciamento de requisitos
A informação é acessível aos usuários interessados	Segurança da informação referente a acessos e privilégios Controle de autorizações
Há um sistema de controle interno sobre relatórios financeiros	Avaliação de riscos de TIC Gestão da qualidade Planos de desastres e recuperação

Impacto da SOX e a Governança de TIC

Segundo Fernandes e Abreu (2012), o CIO (“Chief Information Officer”) é peça fundamental no esforço da empresa para que esta se adeque à SOX, pelo plano de TIC, devendo participar ativamente do projeto de adequação, que deve contemplar os seguintes itens:

- Implantação de novas aplicações e de novos controles em aplicações legadas;
- Ajuste de processos de TIC já existentes e criação de novos processos visando à mitigação de riscos;
- Adequação na estrutura organizacional da área de TIC em função dos ajustes nos processos;
- Definição e implementação de indicadores de desempenho;
- Monitoração constante dos riscos de TIC.

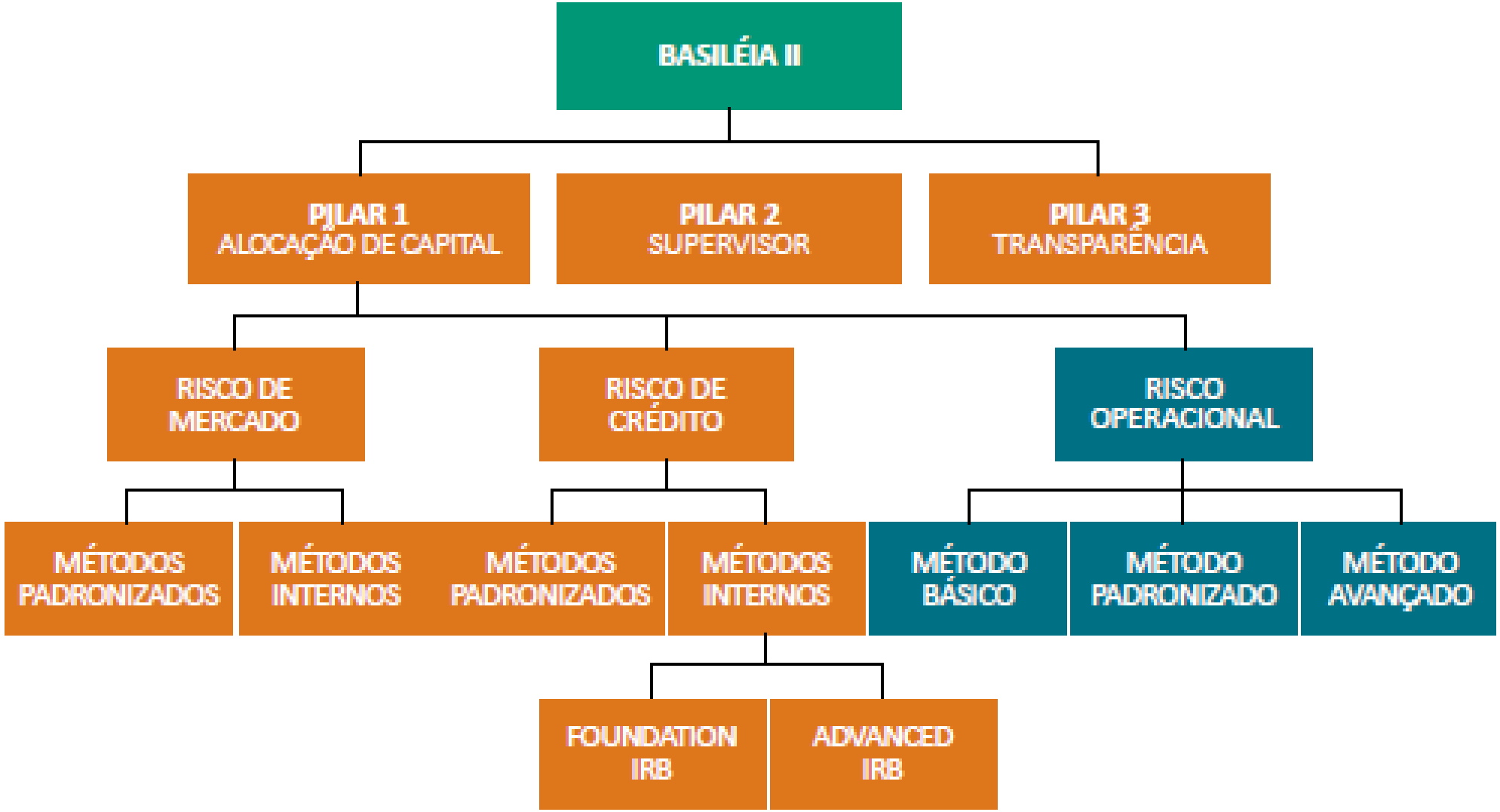
Regulamentações de conformidade com Basileia II

Visando a reduzir a exposição das instituições financeiras e preservar sua solidez, o Acordo da Basileia II estipula requisitos de capital mínimo, em função de riscos de crédito e operacionais.

Está fundamentado em três pilares:

- O cálculo dos requisitos de capital, em função de riscos de crédito e operacionais, sendo que risco de crédito é a perda, pela instituição financeira, causada pela incapacidade do tomador de recursos honrar seus compromissos, e risco operacional expressa a possibilidade de perdas financeiras resultantes de processos internos inadequados;
- Os Bancos Centrais dos países podem realizar auditorias nas instituições financeiras, avaliando os processos de gestão de riscos de crédito e operacionais, assim como a emissão de informações para o mercado em relação à situação de risco das instituições financeiras;
- Existem regras para a comunicação para o mercado dos requisitos mínimos de capital,

Regulamentações de conformidade com Basileia II



Fonte Site da Febraban, artigo técnico de Demerval Bicalho Carvalho e Marcelo Petroni Caldas. Disponível em: www.febraban.org.br/Arquivo/Serviços/Imprensa/Artigo_BasileiaII.pdf>.

Implicações do Acordo da Basileia II sobre a TIC

O Acordo da Basileia II abrange praticamente todos os processos de TIC e áreas organizacionais. Os principais processos de TIC afetados são:

- Capacidade de armazenamento de informações e planejamento da capacidade;
- Integridade das informações de transações do banco e do cliente e de suas transações, também do processo de emissão de relatórios exigidos pela auditoria do Acordo;
- Segurança das informações;
- Planos de continuidade de negócios e de desastres e recuperação de informações.

- As responsabilidades do CIO, através de seu Plano de TIC, são:
- Implantação de novos processos de TIC e ajuste dos existentes;
- Adequação na estrutura organizacional da área de TIC em função dos ajustes nos processos;
- Definição e implantação de indicadores de desempenho;
- Tratamento dos riscos relacionados à TIC para o negócio como um processo.

O Banco Central do Brasil exerce auditorias nas áreas de TIC dos bancos através do framework do Cobit, que será objeto de intenso estudo nas próximas aulas. Como o mercado bancário brasileiro é um dos mais sofisticados do mundo em termos de automação dos processos de negócio e a dependência para a TIC é significativa, o risco operacional da TIC para o negócio deve ser tratado criteriosamente.

Considerações finais

Podemos concluir, portanto, que a Governança de TIC é fundamental para as organizações poderem atender as demandas regulatórias específicas de seus mercados de atuação.

Dentre as exigências regulatórias mais abrangentes, estão a Lei Sarbanes-Oxley, ligada às empresas de capital aberto que possuem ações na Bolsa de Valores americana ou das subsidiárias de empresas americanas de capital aberto pelo mundo. A SOX faz referência às exigências sobre os relatórios financeiros, exigindo processos de controle para garantir integridade das informações, segregação de acessos, inexistência de fraudes e outros aspectos, estabelecendo penalidades na esfera civil e criminal aos executivos das empresas, destacadamente ao CIO e ao CFO, responsáveis pelos resultados financeiros e regulamentando e certificando as empresas de auditoria a aplicar seu escopo nas empresas.

Outra exigência regulatória importante vem do Acordo da Basileia II, voltado somente a instituições financeiras, que estabelece processos de controle para mitigar riscos de crédito e operacionais, e estabelece padrões de auditorias que verifiquem a aderência a esses processos de controle e divulguem os resultados da exposição ao risco por parte das instituições financeiras.

Em ambos os casos, a área de TIC é altamente comprometida no sentido em que os riscos operacionais estejam ligados à execução dos processos de TIC. Como as empresas sujeitas a SOX e a Basileia têm seus processos de negócio altamente automatizados, os riscos da TIC para o negócio devem ser claramente identificados e tratados, através de controles internos aplicados sobre um conjunto de processos de TIC que envolve segurança das informações, disponibilidade, capacidade de armazenamento e de recuperação de informações.

O CIO exerce papel fundamental, pois é responsável, através de seu Plano de TIC, por garantir que esse processo de gestão dos riscos da TIC para o negócio funcione com excelência dentro da organização.

Referências

CARVALHO, D.B.; CALDAS, M.P. Basileia II: abordagem prática para acompanhamento de risco operacional em instituições financeiras. **Resenha BMF**, São Paulo, p. 76-84. Disponível em <https://www.febraban.org.br/Arquivo/Servicos/Imprensa/Artigo_BasileiaII.pdf>. Acesso em: Acesso em: 20 jan. 2015.

FERNANDES, A. A; ABREU, V. F. **Implantando a governança de TIC**: entendendo as implicações do Sarbanes-Oxley Act. Rio de Janeiro: Brasport , 2012.

TAROUCO, H. H.; GRAEMI, A. R. Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias. **R.Adm.**, São Paulo, v. 46, n. 1, p. 7-18, jan./fev./mar. 2011. Disponível em: <http://www.revistas.usp.br/rausp/ article/view/44521/48141>. Acesso em: 20 jan. 2015.

Site da Febraban (http://www.febraban.org.br).