ABDE
ASSOCIAÇÃO BRASILEIRA
DE DESENVOLVIMENTO

Avaliação de controles internos

COSO – Internal Control Integrated Framework

Marcelo Fridori

- Diretor financeiro do IIA Brasil
- Gerente executivo de auditoria interna da BR Distribuidora
- Certificado pelo IIA – The Institute of Internal Auditors: Certified Internal Auditor, Certified in Control Self-Assessment e Certified in Risk Management Assessment.
- Especialista em Governança, Riscos e Compliance pela KPMG – Risk University Advanced.

Agenda

- COSO – controle interno
- Avaliação de controle interno

COSO

- Em 1985, o COSO (Committee of Sponsoring Organizations of the Treadway Commission) foi constituído para estudar formas para evitar fraudes contábeis.
- Composição (associações norte-americanas):

Principais obras do COSO

- Principais obras:
- 1992: Internal Control – Integrated Framework
- 1996: Internal Control Issues in Derivatives Usage
- 1999: Fraudulent Financial Reporting: 1987-1997
- 2004: Enterprise Risk Management – Integrated Framework
- 2006: Internal Control over Financial Reporting – Guidance for Smaller Public Companies
- 2009: Guidance on Monitoring Internal Control Systems
- 2010: Fraudulent Financial Reporting: 1998-2007
- 2010: Announced a project to update its 1992 Internal Control – Integrated Framework.
- 2013: Internal Control – Integrated Framework
- 2017: Enterprise Risk Management

COSO ICIF

O que não mudou:

- Definição principal de controle interno
- Três categorias de objetivos e cinco componentes de controle interno
- Cada um dos cinco componentes de controle interno são requeridos para um controle interno efetivo
- Importante papel do julgamento no desenho, implementação e condução do controle interno e avaliação de sua efetividade.

O que mudou:

Atualização para mudanças no negócio e ambientes operacionais

Expansão dos objetivos de operações e divulgação

Conceitos fundamentais implícitos permeando os cinco componentes codificados como 17 princípios

Atualizado para o aumento da relevância e dependência de TI

Endereçar avaliação do risco de fraude e respostas a esse risco.

Definição de controle interno

- Controle é um processo conduzido pela estrutura de governança, pela administração e por outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.

Definição de controle interno

Definição de controle interno	Complemento
Conduzido para atingir objetivos...	Os objetivos são atingidos em uma ou mais categorias separadas, porém sobrepostas (operacional, divulgação e conformidade).
Um processo...	Um processo que consiste em tarefas e atividades contínuas.
Realizado por pessoas	Não se tratam simplesmente de um manual de políticas e procedimentos, sistemas e formulários, mas diz respeito às pessoas e às ações que elas tomam em cada nível da organização para realizar o controle interno.
Segurança razoável	Capaz de proporcionar segurança razoável, mas não absoluta, para a estrutura de governança e alta administração de uma entidade.
Adaptável à estrutura da entidade	Flexível na aplicação, para toda a entidade ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular.

Cinco componentes e 17 princípios devem estar presentes e em funcionamento

Ambiente de controle

- Conjunto de padrões, processos e estruturas que fornecem a base de implantação do controle interno através da organização. O Conselho de Administração e a Alta Administração estabelecem a importância do controle interno, incluindo padrões de conduta esperados.
- A administração reforça as expectativas nos vários níveis da organização. O Ambiente de Controle abrange a integridade e valores éticos da organização: os parâmetros que permitem ao Conselho de Administração implantar sua supervisão quanto à responsabilidade de governança; estrutura organizacional, delegação de autoridades e responsabilidades; processo para atração, desenvolvimento e retenção de indivíduos competentes; e o rigor em torno da medição de performance, incentivos, e recompensas para direcionar a prestação de contas por performance.
- O Ambiente de Controle resultante tem um impacto profundo em todo o sistema de Controle Interno.

Ambiente de controle

Ambiente de Controle é a fundação para um sistema de Controle Interno.

Esclarece orientação quanto a:

- Papel da Governança numa organização, reconhecendo diferenças nas estruturas, requerimentos e desafios através de diferentes jurisdições, setores e tipos de entidades
- Expectativas de integridade e valores éticos
- Supervisão do risco e fortalecimento das ligações entre risco e performance a fim de ajudar na alocação de recurso para suportar a auditoria interna
- Necessidade em considerar controle interno através da organização expandida, resultante de modelos diferentes de negócio, uso de provedores de serviços terceirizados e outros parceiros externos

Ambiente de Controle: Princípio # 1

1. A organização demonstra comprometimento com a integridade e os valores éticos

- Estabelece o “Tom no Topo”
- Estabelece padrões de conduta
- Avalia aderência aos “Padrões de Conduta”
- Endereça desvios de maneira tempestiva

Ambiente de Controle: Princípio # 2

2. A estrutura de governança demonstra independência em relação aos executivos e supervisiona o desenvolvimento e o desempenho do controle interno.

- Definição das responsabilidades de supervisão
- Aplicação de conhecimento especializado
- Opera independentemente
- Supervisão do Sistema de controles internos

Ambiente de Controle: Princípio # 3

3. Administração estabelece, com a supervisão do Conselho, estruturas, linhas de reporte, limites de autoridade e responsabilidades apropriados na busca dos objetivos

- Considera toda a estrutura da entidade
- Definição de linhas de subordinação
- Definição e limites de autoridade e responsabilidade

Ambiente de Controle: Princípio # 4

4. A organização demonstra comprometimento para atrair, desenvolver e reter talentos competentes, em linha com seus objetivos.

- Estabelece políticas e práticas
- Avaliação de competências e resolução de desvios
- Recrutamento, desenvolvimento e retenção de profissionais
- Plano de sucessão

Ambiente de Controle: Princípio # 5

5. A organização faz com que as pessoas assumam responsabilidade por suas funções de controle interno na busca pelos objetivos.

- Prestação de contas por meio de estruturas, autoridades e responsabilidades
- Definição de medidas de desempenho, incentivos e recompensas
- Avaliar o desempenho e recompensar ou disciplinar as pessoas

Compromisso com a integridade

Componente	**Ambiente de Controle**		
Princípio	1. A organização demonstra o compromisso com a integridade e os valores éticos.		
Controles das **Linhas de Defesa e de outros princípios e componente s** devem operar de forma integrada	Dissemina em toda a organização os valores éticos e os padrões de conduta.	Assessora a Administração na implantação de programas de integridade.	Avalia o desenho, a implantação e a eficácia dos programas e atividades relacionados com os padrões éticos da organização.
	Administração	*Riscos e Compliance*	*Auditoria Interna*

Avaliação de risco

- Envolve um processo dinâmico para identificação e avaliação dos riscos de realização dos objetivos. Riscos de toda a entidade são considerados e relacionados com a tolerância estabelecida. Portanto, a avaliação de risco forma a base para se determinar como os riscos serão gerenciados.

- A administração especifica objetivos relacionados às operações, ao reporte e à conformidade com suficiente clareza a fim de ser capaz de identificar e analisar os riscos relacionados com estes objetivos. A avaliação de risco requer da administração a consideração do impacto de possíveis mudanças no ambiente externo, bem como dentro de seu próprio negócio, que possam acarretar em um controle interno ineficaz.

Avaliação de risco

Avaliação de Risco – Mudanças Framework 2013

Esclarece que a avaliação de risco inclui processos para identificação de risco, análise de risco e resposta ao risco

- Amplia a discussão sobre:
- tolerância ao risco (níveis de risco aceitáveis) e que o risco pode ser gerenciado através das seguintes respostas: aceitar, evitar ou compartilhar o risco
- necessidade do entendimento das mudanças significativas em fatores internos e externos, bem como análise do impacto no sistema de controle interno
- Inclui como parte do processo de avaliação de risco uma avaliação específica do risco de fraude relacionado a erros ou omissões materiais nas DFs, salvaguarda inadequada de ativos e corrupção

Avaliação de Risco: Princípio # 6

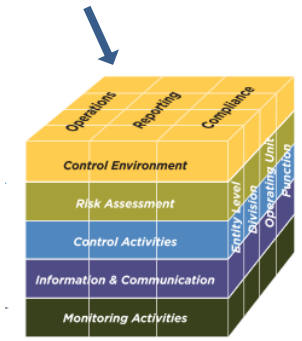
6. A organização especifica os objetivos com clareza suficiente a fim de permitir a identificação e a avaliação dos riscos associados.

- Segrega características relacionadas a: operações; reportes financeiros externos; reportes não-financeiros externos; reportes internos; objetivos de conformidade

Avaliação de Risco: Princípio # 6

6. A organização especifica os objetivos com clareza suficiente a fim de permitir a identificação e a avaliação dos riscos associados.

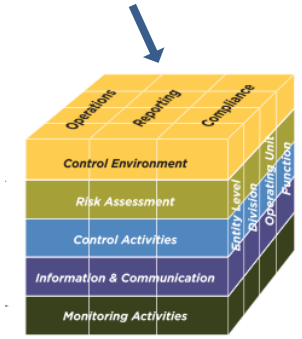
- Objetivos de Operações
  - Reflete as escolhas da administração
  - Considera a tolerância ao risco
  - Inclui metas de desempenho operacionais e financeiras
  - Forma uma base para o comprometimento de recursos



Avaliação de Risco: Princípio # 6

6. A organização especifica os objetivos com clareza suficiente a fim de permitir a identificação e a avaliação dos riscos associados.

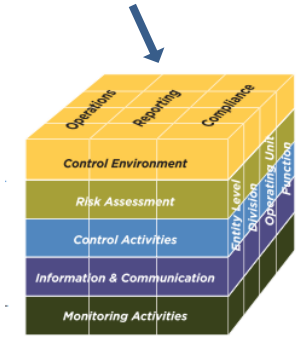
- Objetivos de relatórios (externos) financeiros
  - Conformidade com normas de contabilidade aplicáveis
  - Considera a materialidade
  - Reflete atividades da entidade/organização



Avaliação de Risco: Princípio # 6

6. A organização especifica os objetivos com clareza suficiente a fim de permitir a identificação e a avaliação dos riscos associados.

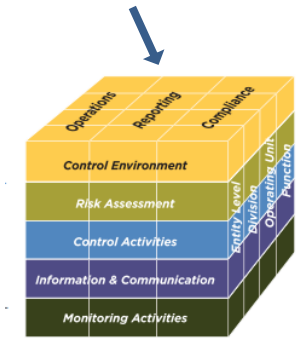
- Objetivos de relatórios (externos) não financeiros
  - Conformidade com normas e estruturas estabelecidas
  - Considera o nível de precisão requerido
  - Reflete atividades da entidade/organização



Avaliação de Risco: Princípio # 6

6. A organização especifica os objetivos com clareza suficiente a fim de permitir a identificação e a avaliação dos riscos associados.

- Objetivos de relatórios internos
  - Reflete decisões da administração
  - Considera o nível de precisão requerido
  - Reflete atividades da entidade/organização



Avaliação de Risco: Princípio # 6

6. A organização especifica os objetivos com clareza suficiente a fim de permitir a identificação e a avaliação dos riscos associados.

- Objetivos de compliance
  - Reflete as leis e a regulamentação
  - Considera a tolerância ao risco

Avaliação de Risco: Princípio # 7

7. A organização identifica os riscos à realização de seus objetivos por toda a entidade e analisa os riscos como uma base para determinar a forma como devem ser gerenciados.

- Análise de fatores internos e externos.
- Estimativa da relevância dos riscos identificados.
- Definição da resposta aos riscos.

Avaliação de Risco: Princípio # 8

8. A organização considera o potencial de fraude na avaliação de riscos para o alcance dos objetivos

- Considera diversos tipos de fraude
- Avalia incentivos e pressões
- Avalia oportunidades
- Avalia atitudes e racionalizações

Avaliação de Risco: Princípio # 9

9. A organização identifica e avalia mudanças que poderiam impactar significativamente o sistema de controle interno

- Avalia mudanças no ambiente externo
- Avalia mudanças no modelo de negócio
- Avalia mudanças na liderança

Avaliação de risco

Componente	**Avaliação de Riscos**		
Princípio	8. A organização considera o potencial de fraude na avaliação dos riscos de não realização dos objetivos.		
Controles das **Linhas de Defesa e de outros princípios e componente s** devem operar de forma integrada	Implanta e opera um processo para captação e tratamento de denúncias de irregularidades, assegurando a confidencialidade dos denunciantes.	Utiliza as informações das denúncias procedentes na revisão das avaliações dos riscos de fraude.	Avalia de forma independente o Ambiente de Controle, considerando as averiguações e respectivas ações corretivas dos gestores.
	Administração	*Riscos e Compliance*	*Auditoria Interna*

Atividades de controle

- Atividades de Controle são as ações estabelecidas através de políticas e procedimentos para mitigar os riscos na realização dos objetivos.
- Atividades de Controle são efetuadas em todos os níveis da entidade, em vários estágios dentro dos processos de negócio e sobre o ambiente tecnológico. Estas devem ser preventivas ou detectivas em sua natureza e devem envolver uma variedade de atividades manuais e automáticas tais como autorizações e aprovações, verificações, reconciliações e revisões de performance do negócio.
- Segregação de funções é tipicamente construída dentro da seleção e desenvolvimento das atividades de controle. Onde a segregação de funções não é possível, a administração deve selecionar e desenvolver atividades de controle alternativas.

Atividades de controle

- Atividades de Controle - Mudanças Framework 2013
- Atualiza-se com a evolução na tecnologia desde 1992 (ex.: substitui os conceitos de datacenter com uma discussão mais geral sobre infraestrutura de tecnologia)
- Endereça ligação entre processos de negócio, atividades de controle automatizadas e GITCs
- Contrasta controles em nível de transação de controles em outros níveis da organização
- Atualiza a aplicação de GITCs (infra-estrutura de TI; gerenciamento de segurança; aquisição de tecnologia; desenvolvimento e manutenção) sobre todas as plataformas tecnológicas
- Esclarece que atividades de controle são ações estabelecidas por políticas e procedimentos ao invés de ser apenas políticas e procedimentos

Atividades de controle: Princípio # 10

10. A organização seleciona e desenvolve atividades de controle que contribuem na mitigação de riscos em níveis aceitáveis.

- Integra-se com Avaliação de Risco
- Considera fatores específicos da entidade
- Determina processos relevantes do negócio
- Avalia a combinação de tipos de controle
  - Atividades de Controle incluem uma variedade de controles, considerando tanto controles manuais e automáticos, controles preventivos e detectivos.
  - Considera em que nível os controles são aplicados
  - Endereça segregação de funções

Atividades de controle: Princípio # 11

11. A organização seleciona e desenvolve atividades de controle gerais sobre tecnologia para suportar a realização dos objetivos.

- Determina grau de dependência entre o uso de tecnologia nos processos de negócio e controles gerais de tecnologia
- Estabelece atividades de controle relevantes de Infraestrutura de Tecnologia as quais são desenhadas e implementas para ajudar a precisão e a disponibilidade do processamento de tecnologia
- Estabelece atividades de controle relevantes do Processo de Gerenciamento da Segurança as quais são desenhadas e implementadas a fim de restringir privilégios de acesso a tecnologia para usuários autorizados adequados com suas responsabilidades e proteger os ativos da entidade de ameaças externas
- Estabelece aquisição, desenvolvimento e manutenção de tecnologia. Administração seleciona e desenvolve atividades de controles sobre aquisições, desenvolvimento e manutenção de tecnologia e sobre sua infraestrutura para a realização dos objetivos.

Atividades de controle: Princípio # 12

12. A organização implanta atividades de controle através de políticas, que estabelecem o que é esperado, e através de procedimentos, que colocam as políticas em ação

- Estabelece políticas e procedimentos para suportar a implantação das diretrizes da Administração
- Estabelece responsabilidade e prestação de contas na execução de políticas e procedimentos
- Executa de maneira tempestiva
- Toma ação corretiva
- Os controles internos são executados por funcionários competentes
- Reavaliam políticas e procedimentos

Atividades de controle

Componente	**Atividades de Controle**		
Princípio	10. A organização seleciona e desenvolve atividades de controle que contribuem na mitigação de riscos em níveis aceitáveis para a realização dos objetivos.		
Controles das **Linhas de Defesa e de outros princípios e componentes** devem operar de forma integrada	Possui responsabilidade direta pelo sistema de controle interno e por identificar as mudanças que poderiam impactá-lo significativamente.	Monitora regularmente e considera mudanças nos riscos da organização relacionados com os aspectos legais, regulatórios e de *compliance*.	Certifica que os controles implantados pela Administração foram projetados de forma apropriada, implantados com eficácia e operam conforme previsto.
	Administração	*Riscos e Compliance*	*Auditoria Interna*

Informação e comunicação

- Informação é necessária para a entidade na execução das responsabilidades de controle interno para suportar a realização de seus objetivos.
- Administração obtém/ gera relevante informação com qualidade, de fontes internas e externas, para suportar o funcionamento de outros componentes de controle interno.
- Comunicação é um processo contínuo, interativo que provê, compartilha e obtêm informações necessárias.
- Comunicação Interna é o meio pelo qual informação é disseminada pela organização, fluindo através da entidade. Isso possibilita aos funcionários receber uma mensagem clara da alta administração que as responsabilidades de controle devem ser levadas a sério.
- Comunicação externa tem duas faces: possibilita entrada da comunicação de informação externa relevante e provê informação para partes externas em resposta a requerimentos e expectativas.

Informação e comunicação

- Mudanças Framework 2013
- Enfatiza a importância da qualidade da informação
  - Incluindo como a entidade gerencia informação e comunicação com provedores de serviço terceirizados, bem como com aqueles que operam fora de seus limites operacionais e legais.
- Expande a discussão em:
  - Impacto dos requerimentos regulatórios na confiança e proteção da informação
  - Volume e fontes de informação, tendo em conta o aumento da complexidade dos processos de negócio, maior interação com partes externas e avanços tecnológicos
- Reflete o impacto da tecnologia e outros mecanismos de comunicação em sua velocidade, meios e qualidade no fluxo de informações

Informação e Comunicação: Princípio # 13

13. A organização obtém ou gera e utiliza informação relevante e de qualidade para apoiar o funcionamento do controle interno

- Identifica requerimentos da informação
- Capta dados de fontes internas e externas
- Processa dados relevantes em informações
- Mantém qualidade em seu processamento

Informação e Comunicação: Princípio # 14

14. A organização transmite internamente as informações necessárias para apoiar o funcionamento do controle interno, inclusive os objetivos e responsabilidades pelo controles

- Comunica-se com a estrutura de governança
- Fornece linhas independentes de comunicação
- Seleciona métodos de comunicação relevantes

Informação e Comunicação: Princípio # 15

15. A organização comunica-se com os públicos externos sobre assuntos que afetam o funcionamento do controle interno.

- Comunica-se com os públicos externos
- Possibilita o recebimento de comunicações
- Comunica-se com a estrutura de governança

Atividades de Monitoramento

- Avaliações contínuas, avaliações específicas independentes, ou uma combinação das duas, são utilizadas para determinar se cada um dos cinco componentes de controle interno, incluindo controles que afetam os princípios dentro de cada componente, estão presentes e em funcionamento.
- Avaliações contínuas, incorporadas aos processos de negócio em diferentes níveis da entidade, proveem informações tempestivas. Avaliações específicas, conduzidas periodicamente, irão variar em escopo e frequência, dependendo da avaliação de risco, efetividade das avaliações contínuas e outras considerações da Administração.
- As ocorrências são avaliadas conforme critérios estabelecidos por órgãos reguladores, órgãos normativos ou pela Administração e Conselho de Administração. As deficiências são comunicadas à Administração e ao Conselho de Administração de maneira apropriada.

Atividades de Monitoramento

- Mudanças Framework 2013
- Refina a terminologia. Duas categorias principais de monitoramento de atividades são classificadas como “avaliações contínuas” e “avaliações específicas independentes”
- Inserida a necessidade de uma base de entendimento para o estabelecimento de avaliações contínuas e específicas independentes.
- Expansão da discussão do uso de tecnologia e de prestadores de serviços.

Monitoramento: Princípio # 16

16. A organização seleciona, desenvolve e executa avaliações contínuas e independentes para confirmar se os componentes do controle interno estão presentes e em funcionamento.

- Considera uma combinação de avaliações contínuas e independentes
- Considera o ritmo das mudanças: A administração considera o ritmo de mudanças nos negócios e processos de negócios ao selecionar e desenvolver as avaliações contínuas e separadas.
- Utiliza pessoal com conhecimento
- Integra aos processos de negócios: As avaliações contínuas são inseridas nos processos de negócios e ajustadas quando as condições se modificam.
- Ajusta o escopo e a frequência: A administração varia o escopo e a frequência das avaliações separadas dependendo do risco.
- Avalia objetivamente

Monitoramento: Princípio # 17

17. A organização avalia e comunica deficiências no controle interno em tempo hábil aos responsáveis por tomar ações corretivas, inclusive a estrutura de governança e alta administração, conforme aplicável.

- Avalia resultados
- Comunica deficiências
- Monitora ações corretivas

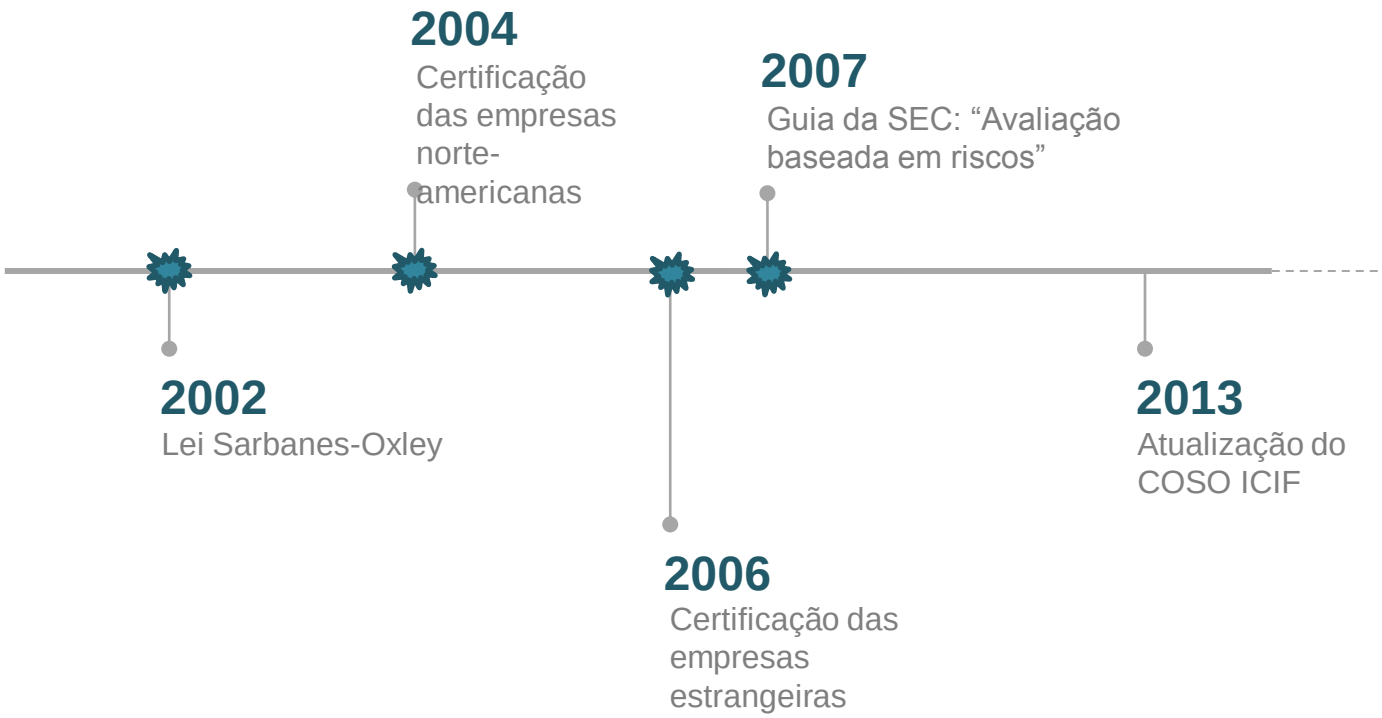
Avaliações independentes

Componente	**Atividades de Monitoramento**		
Princípio	16. A organização seleciona, desenvolve e executa avaliações contínuas e independentes para confirmar se os componentes do controle interno estão presentes e em funcionamento.		
Controles das **Linhas de Defesa e de outros princípios e componentes** devem operar de forma integrada	Reporta periodicamente ao Comitê de Auditoria sobre o desempenho das atividades de controle da organização.	Monitora se o alcance dos objetivos está dentro das tolerâncias estabelecidas para os riscos mapeados.	Certifica que o sistema de controle interno está operando conforme previsto e os riscos são gerenciados respeitando-se a tolerância a riscos da organização.
	Administração	*Riscos e Compliance*	*Auditoria Interna*

ABDE
ASSOCIAÇÃO BRASILEIRA
DE DESENVOLVIMENTO

Avaliação de controles internos

Avaliação de controles internos



Empresas brasileiras listadas na NYSE

Lei Sarbanes-Oxley

A SOX possui 68 seções, com destaque para:

- **Seção 404 – Controles Internos**

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Fases da avaliação

- Identificação dos principais processos
- Mapeamento dos riscos
- Documentação dos controles
  - Narrativa
  - Fluxo
- Avaliação das ações corretivas
- Testes dos controles
- Avaliação das deficiências

Definição dos processos

- Cálculo da materialidade
- Contas contábeis significativas
- Identificação dos processos
- Levantamento das unidades operacionais

Cálculo da materialidade

Critérios relacionados às operações

- Os critérios relacionadas às operações são calculados a partir do Resultado Líquido ajustado antes dos impostos, à razão de 5%, ou a partir da Receita operacional de vendas, à razão de 0,5%.

Critérios relacionados à posição financeira

- Os critérios relacionados à posição financeira são calculados a partir do Ativo Total, à razão de 0,5%, ou a partir do Patrimônio Líquido, à razão de 1,0%.

Identificação dos processos

- Levantamento das contas contábeis significativas conforme cálculo de materialidade
- Devem ser identificados todos os processos que estão diretamente relacionados com cada contábil significativa
- Correlação: Conta Contábil Material x Respectivos Processos

Exemplos de riscos SOx

Processo Compras

- Realização de alterações indevidas no cadastro de fornecedores (inclusão, alteração e exclusão)

Processo Empréstimos e Financiamentos

- Pagamentos de empréstimos não registrados

Controles x riscos

Risco Compras: Alterações do cadastro de fornecedores

- Controles:
  - Mensalmente, a partir do relatório “XPTO”, a gerência da unidade revisa todas as inclusões, alterações e exclusões de fornecedores
  - As alterações dos dados financeiros dos fornecedores são aprovadas pela gerência por meio da transação XYZ do sistema de Contas a Pagar

Risco Empréstimos: Registro dos pagamentos

- Controle:
  - Extratos recebidos de credores são reconciliados com os registros contábeis e as diferenças, resolvidas.

Classificação dos controles

- Riscos mitigados

- Manual / Automático
- Detectivo / Preventivo

- Frequência: diário, semanal, a cada transação, etc

- Objetivos de auditoria (“assertions”)

Categoria de controle

- Autorização
- Configuração
- Relatórios de exceção
- Interface / conversão de dados
- Indicadores chaves de desempenho
- Revisão da administração
- Reconciliação
- Segregação de funções
- Acesso ao sistema

Categoria de controle

Controle	Explicação e Exemplo
Autorização	*Incluem:* - Aprovação das transações executadas de acordo com políticas e procedimentos, gerais ou específicos. - Parâmetros e perfil de acesso do sistema configurado conforme políticas da Empresa. *Exemplo:* Acréscimo/modificações nos arquivos-mestres de empregados (novo empregado, escolha de beneficio, salário inicial e modificações de salário no sistema da folha de pagamentos) são apropriadamente autorizados.
Configuração	*Incluem*: Controles que são desenvolvidos para proteger os dados contra processamento inapropriado e auxiliar na manutenção da integridade dos dados. *Exemplo:* Configuração de sistema evita o cadastramento em duplicidade de clientes. A configuração é desenvolvida, implementada, utilizada, mantida apropriadamente e sujeita a procedimentos de mudança.

Categoria de controle

Controle	Explicação e Exemplo
Relatórios de exceção/edição	*Incluem:* Um relatório gerado por uma entidade para monitorar algum item. Os relatórios podem incluir relatórios de exceções (violações de uma norma estabelecida), de edição (mudança de um arquivo-mestre). *Exemplo:* Relatório de exceção gerado para clientes que excedem seus limites de crédito estabelecidos.
Controle de interface / conversão	*Incluem:* - Interface de dados – a transferência de porções definidas de informação (dados) entre dois sistemas de computadores, utilizando meios manuais ou automatizados. Isto deve garantir a integridade dos dados que estão sendo transferidos. - Dados de conversão – o processo de migração de dados de um sistema anterior (que podem ser dados ultrapassados, duplicados, incorretos, incompletos, os quais residem em várias posições dentro do sistema) para o novo sistema. *Exemplo:* Interface de dados entre o sistema de vendas e razão contábil.

Categoria de controle

Controle	Explicação e Exemplo
Indicadores chave de desempenho (KPI's) – Indicadores de Performance	*Inclui:* A preparação periódica e oportuna, a revisão e a analise dos indicadores chave de desempenho. São mensurações quantitativas, financeiras e não financeiras, que são: - coletadas pela entidade, seja periódica ou continuamente; e - usadas pela administração para avaliar o progresso em relação aos objetivos definidos da entidade. *Exemplo:* A análise de vendas (período corrente e período anterior comparável, orçamentos, etc.,divididos por região, linha de produção, etc.) é realizada regularmente e as variações não usuais são acompanhadas.
Revisão da Administração	*Inclui:* A atividade de uma pessoa, que não o preparador, analisando e supervisionando as atividades executadas. *Exemplo:* Comparação de uma lista de preços antiga com a lista revisada é realizada para assegurar que as mudanças feitas reflitam aquelas que foram autorizadas.

Categoria de controle

Controle	Explicação e Exemplo
Reconciliação	Um controle destinado a verificar se dois itens/sistemas de computador, etc. são consistentes. *Exemplo:* Extratos bancários são reconciliados mensalmente com o razão. Importante: as pendências identificadas nas conciliações devem ser analisadas e justificadas.
Segregação de funções	A segregação de deveres e responsabilidades de autorizar transações, contabilizar transações e manter custódia para evitar que as pessoas estejam numa posição tanto de penetrar como de esconder um erro ou irregularidade. *Exemplo:* Pessoas que aprovam compras não devem ter acesso aos pagamentos.
Acesso ao sistema	A capacidade que usuários ou grupos de usuários têm, dentro de um ambiente de processamento de um sistema de informações computadorizadas, tal como estabelecido e definido por direitos de acesso configurados no sistema. Os direitos de acesso num sistema correspondem ao acesso na prática. *Exemplo:* Acesso para acréscimo/modificação no arquivo-mestre de empregados no sistema de folha de pagamentos é limitado às pessoas apropriadas (perfil de acesso).

Testes dos controles internos

- Ondas de testes durante o ano
- As amostras geradas variam de acordo com os riscos e a periodicidade dos controles e não focam especificamente uma unidade
- Independente da avaliação da Administração (Auditoria Interna), a Auditoria Externa também avalia os controles existentes

Avaliação das falhas

- As falhas identificadas devem ser avaliadas considerando a magnitude dos valores envolvidos e a eventual existência de controles compensatórios.

- Classificar a falha como:

1. Deficiência
2. Deficiência significativa
3. Fraqueza material: Reportar no 20-F a falha e o plano de ação

Exemplo de resultado publicado

B. Relatório da Administração acerca do Controle Interno sobre a Elaboração de Relatórios Financeiros

Nossa administração é responsável por estabelecer e manter controles internos adequados sobre relatórios financeiros.

Com base nestas avaliações e critérios, nossa administração identificou uma deficiência de controle, em 31 de dezembro de 2018, que representa uma fraqueza material em nosso controle interno sobre relatórios financeiros. A ineficácia deste controle interno não resultou em distorção ou omissão em nossas demonstrações financeiras consolidadas em 31 de dezembro de 2018 e no exercício findo naquela data.

Fraqueza Material no Controle Interno sobre relatórios financeiros

Uma fraqueza material é uma deficiência, ou uma combinação de deficiências, no controle interno sobre relatórios financeiros, de tal forma que há uma possibilidade razoável de que uma distorção relevante nas demonstrações contábeis anuais ou intermediárias da empresa não seja evitada ou detectada tempestivamente.

Nossa administração identificou uma conta de serviço (suporte ao sistema ERP) com acesso privilegiado.

Essa conta, se usada incorretamente, poderia permitir o acesso a transações do sistema para a realização de alterações indevidas.

Referências

COSO. Controle interno – estrutura integrada: sumário executivo. IIA Brasil. 2013.

- http://www.iiabrasil.org.br/new/2013/downs/coso/COSO_ICIF_2013_Sumario_Executivo.pdf

COSO. Internal control – integrated framework: executive summary, framework and appendices. North Carolina: 2013.

COSO. Internal control – integrated framework: internal control over external financial reporting: a compendium of approaches and examples. North Carolina: 2013.

IIA - THE INSTITUTE OF INTERNAL AUDITORS. Declaração de posicionamento : As três linhas de defesa no gerenciamento eficaz de riscos e controles. IIA Brasil. 2013.

- http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf

IIA - THE INSTITUTE OF INTERNAL AUDITORS. EvaluatIng ethics-related programs and actIvItIes. 2012.

- https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Evaluating-Ethics-related-Programs-and-Activities-Practice-Guide.aspx

IIA - THE INSTITUTE OF INTERNAL AUDITORS. Leveraging COSO across the three lines of defense. 2015.

- http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf

Obrigado!

Marcelo Fridori
(11) 5523-1919
Marcelo.Fridori@iiabrasil.org.br