INSTITUTO SERZEDELLO CORRÊA

AVALIAÇÃO DE CONTROLES INTERNOS

AULA 2:
MODELOS DE REFERÊNCIA PARA CONTROLE INTERNO

JUNHO, 2012

RESPONSABILIDADE PELO CONTEÚDO

Tribunal de Contas da União

Secretaria Geral da Presidência

Instituto Serzedello Corrêa

2ª Gerência de Desenvolvimento de Competências

Serviço de Planejamento e Projetos Educacionais

SUPERVISÃO

Pedro Koshino

CONTEUDISTAS

Antonio Alves de Carvalho Neto

Bruno Medeiros Papariello

TRATAMENTO PEDAGÓGICO

Leonardo Pereira Garcia

PROJETO GRÁFICO

Ismael Soares Miguel

Paulo Prudêncio Soares Brandão Filho

Bianca Novais Queiroz

NORMALIZAÇÃO

Kélem Cristina Amaro dos Santos

Patrícia Paula Giovanna de Souza Ferreira

Denise Curcio dos Santos

DIAGRAMAÇÃO

Vanessa Vieira

Brasil. Tribunal de Contas da União.

Curso de avaliação de controles internos / Tribunal de Contas da União; Conteudistas: Antonio Alves de Carvalho Neto, Bruno Medeiros Papariello. 2. ed. – Brasília : TCU, Instituto Serzedello Corrêa, 2012.

56 p.

Aula 2. Modelos de referência para controle interno.

1. Controle interno, avaliação, estudo e ensino. I. Carvalho Neto, Antonio Alves de. II. Papariello, Bruno Medeiros. III. Programa de aprimoramento profissional em auditoria PROAUDI). IV. Título.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

Aula 2 - Modelos de referência para controle interno

Existem modelos que podem ser usados como referência para implementação e avaliação de controles internos?

Qual o modelo mais utilizado mundialmente?

Quais são as principais normas e regulamentações sobre controle interno que têm influência no Brasil?

Para responder a essas e a outras questões apresentaremos, nesta aula, as principais abordagens metodológicas relativas ao controle da gestão organizacional no que diz respeito à governança, aos modelos de gestão de riscos e controles internos e em relação à tecnologia da informação.

Também apresentaremos as mais importantes regulamentações e normas legais relacionadas ao tema, em nível internacional e aplicadas no Brasil.

Em seguida, abordaremos os elementos de um sistema de controle interno eficaz, baseando-nos no modelo Coso II, pois este, além de incorporar o modelo Coso I, aborda a gestão de riscos organizacionais.

Os conceitos trabalhados nesta aula são fundamentais para a compreensão e realização de avaliações tanto em nível da entidade como um todo ou em partes dela, que será estudada na aula 3, quanto em nível de atividades ou processos organizacionais específicos, que será estudada na aula 4.

Sumário

Para facilitar o estudo, esta aula está organizada da seguinte forma:

Ao final desta aula, esperamos que você tenha condições de:

- diferenciar os modelos de referência e as regulamentações de controle interno reconhecidos internacionalmente;
- identificar os elementos de um sistema de controle interno eficaz;
- definir critérios para compor uma estrutura de controle interno a partir dos modelos de referência estudados, para servir de base para avaliação do controle interno em nível de entidade.

Lista de Siglas

AICPA - *American Institute of Certified Public Accountants* (Instituto Americano de Contadores Públicos Certificados)

BID - Banco Interamericano de Desenvolvimento.

BIS - *Bank for International Settlements*

CFC – Conselho Federal de Contabilidade

CMN - Conselho Monetário Nacional

CobiT - *Control Objectives for Information and Related Technology*

Coso - *Committee of Sponsoring Organizations of The Treadway Commission* (Comitê das Organizações Patrocinadoras da Comissão Tradway)

DN-TCU - Decisão Normativa TCU

EFS - Entidade de Fiscalização Superior

GAO - *Government Accountability Office*. Instituição Suprema de Auditoria dos EUA.

Ifac - *International Federation of Accountants* (Federação Internacional de Contadores – EUA)

IIA - *The Institute of Internal Auditors* (Instituto dos Auditores Internos)

Intosai - *International Organization of Supreme Audit Institutions* (Organização Internacional das Entidades de Fiscalização Superior)

ISA - *International Standards on Auditing* (Normas Internacionais de Auditoria)

Isaca - *Information Systems Audit and Control Association*

Itil - *Information Technology Infrastructure Library*

NBC – Norma Brasileira de Contabilidade

OGC - *Office for Government Commerce*

PCAOB - *Public Company Accounting Oversight Board*

SAI - *Supreme Audit Institution* (Entidade de Fiscalização Superior)

SFC - Secretaria Federal de Controle da Controladoria Geral da União

SOX - Lei Sarbanes-Oxley (EUA, 2002)

TCU - Tribunal de Contas da União. Entidade de Fiscalização Superior do Brasil

1. Modelos de referência reconhecidos

A implantação de um determinado conjunto de controles sem a observância de modelos reconhecidamente aceitos pode levar a organização a aparelhar-se com uma coleção de instrumentos e procedimentos burocráticos, descoordenados, que mais dão a falsa impressão da existência de um sistema de controle interno do que garantam efetivamente os benefícios desejados, o que resulta não só em desperdício de tempo e recursos, mas também numa indesejável concentração de poder e influência em quem os administra.

Vimos, na primeira aula deste curso, que o controle interno é um instrumento de gerenciamento de riscos indispensável à governança corporativa. De fato, como cabe à governança assegurar que os recursos da organização sejam empregados de maneira eficaz na consecução da missão e na realização dos objetivos e metas estabelecidos, ela deve cercar o gerenciamento desses recursos com um sistema de controle que atenda suas necessidades específicas (MARTINS; SANTOS; DIAS FILHO, 2004), porém, **que modelo utilizar**?

Nesta aula, abordaremos os modelos de referência mais reconhecidos para implementação e avaliação de controles internos, também denominados modelos estruturais, frameworks ou estruturas de controle interno. Geralmente, as organizações não estabelecem estruturas de controle interno a partir de uma única referência, mas sim combinando abordagens conceituais e preceitos de mais de um modelo, conforme a aderência às suas necessidades, resultando em um sistema de controle interno dimensionado na proporção requerida pelos riscos e em consonância com a natureza, complexidade, estrutura e estratégia envolvidos na consecução dos objetivos que dão suporte à sua missão.

1.1 O modelo Coso I

Em 1985, devido a uma crescente onda de falências de empresas, causando enormes prejuízos aos investidores e à sociedade, o Congresso americano resolveu criar um subcomitê especial para analisar diversos casos que levantavam dúvidas sobre a conduta das administrações das empresas, a adequação dos relatórios financeiros e a efetividade das auditorias independentes.

Na mesma ocasião, diversas entidades profissionais americanas uniram esforços e criaram uma comissão especial – a *Treadway Comission* – com o objetivo de identificar os fatores que permitiam a

produção de relatórios financeiros fraudados e de recomendar medidas para a redução de sua incidência.

Em 1987, a Comissão emitiu um relatório no qual fez uma série de recomendações e conclamou as organizações patrocinadoras da *Treadway Comission* a integrar os diversos conceitos de controle interno e a desenvolver um referencial comum para estabelecer e avaliar controles internos.

Como consequência, em 1992, o Coso (abreviatura de Comitê das Organizações Patrocinadoras) publicou o modelo ***Internal Control – Integrated Framework*** (Controle Interno – Estrutura Integrada), conhecido como **Coso I**, trazendo critérios práticos, amplamente aceitos, para o estabelecimento de controles internos e para a sua avaliação.

O Coso I deu nova dimensão ao papel do controle interno.

O modelo mudou o conceito tradicional de "controles internos" e chamou a atenção para o fato de que eles tinham de fornecer proteção contra riscos, pois, ao definir **risco** como a **possibilidade que um evento ocorra e afete de modo adverso o alcance dos objetivos da entidade**, introduziu a noção de que controles internos devem ser ferramentas de gestão e monitoramento de riscos em relação ao alcance de objetivos, e não apenas dirigidos para riscos de origem financeira ou vinculados a resultados escriturais. **O papel do controle interno foi, assim, ampliado**.

Segundo Borges (apud DAVIS; BLASCHEK, 2006, p. 11) as administrações públicas de países do chamado primeiro mundo, detentores dos níveis mais baixos de fraude e mais altos de pesquisa em gestão pública, seguiram a tendência indicada pelo Coso I, desenvolvendo e utilizando padrões de estrutura de controle interno com esse papel ampliado. Assim, modelos de controle interno utilizando o gerenciamento de riscos na sua base conceitual passaram a ser desenvolvidos e utilizados por diversos países, como o *Cadbury* no Reino Unido, o *CoCo* no Canadá, a *Standard AZ/NZS 4360-1999* na Austrália/Nova Zelândia e o *King Report* na África do Sul, e têm sido um enorme marco no progresso da auditoria interna e da governança nesses países (McNAMEE; SELIM apud DAVIS; BLASCHEK, 2006).

No que diz respeito a entidades ligadas ao setor público, vários organismos internacionais, como o BID e o Banco Mundial, adotaram o modelo Coso. A Intosai, em 2004, atualizou as *Diretrizes para as Normas de Controle Interno do Setor Público* (INTOSAI GOV 9100, 2004) adotando o modelo e, depois, em 2007, incorporou o modelo Coso II, publicando a INTOSAI GOV 9130, 2007.

Diamond (apud DAVIS; BLASCHEK, 2006) destaca que a Intosai

adotou um paradigma mais proativo para os controles internos e para a atuação das auditorias internas governamentais. A auditoria interna, nesse novo paradigma, passou a exercer um papel mais voltado para a avaliação abrangente dos controles internos, com mais ênfase em controles gerenciais e de gerenciamento de riscos, deixando de lado a função de mero avaliador da conformidade legal das despesas públicas.

O TCU, sendo membro da Intosai, também reconhece e utiliza o modelo Coso, adotando como base para suas avaliações de controle interno as normas emitidas pela instituição, ou seja, a INTOSAI GOV 9100, de 2004, e a INTOSAI GOV 9130, de 2007.

No setor privado, várias organizações profissionais internacionais revisaram suas normas para incorporar o modelo introduzido pelo Coso I.

A Federação Internacional de Contadores (Ifac), que emite as Normas Internacionais de Auditoria (ISA), incorporou todos os elementos introduzidos pelo Coso na norma denominada *Matter 400 – Risk Assessments and Internal Control* (Avaliações de Risco e Controle Interno). Essa norma foi posteriormente incorporada na ISA 315 e na ISA 330, ambas adotadas no Brasil, para uso em auditorias independentes do setor privado, por intermédio das Normas Brasileiras de Contabilidade NBC TA 315 e NBC TA 330, aprovadas pelas resoluções nº 1.212/2009 e 1.214/2009, do Conselho Federal de Contabilidade.

O Instituto Americano de Contadores Públicos Certificados (AICPA) emitiu a norma de auditoria SAS 78, substituindo a definição de controle interno da SAS 55 pela definição do Coso I, incorporando os componentes e demais conceitos da estrutura. Isso fez com que o modelo se tornasse paradigma no mercado, pois os auditores passaram a utilizá-lo como padrão para revisão do controle interno em seus trabalhos de auditoria independente.

O Comitê de Basiléia publicou, em 1998, o documento denominado *Framework for Internal Control Systems in Banking Organizations*, no qual enfatiza os cinco componentes do modelo Coso I.

O modelo Coso I tornou-se referência mundial, pelo fato de:

- uniformizar definições de controle interno;
- definir componentes, objetivos e objetos do controle interno em um modelo integrado;
- delinear papéis e responsabilidades da administração;
- estabelecer padrões para desenho e implementação;
- criar um meio para monitorar, avaliar e reportar controles internos.

1.2 O modelo Coso II

A ampla adesão ao modelo Coso I não foi suficiente para estancar escândalos econômico-financeiros e contábeis envolvendo organizações de todos os portes, que sucumbiam de uma hora para outra. A série de escândalos e quebras de negócios de grande repercussão fez com que o Coso encomendasse o desenvolvimento de uma estratégia, que fosse de fácil utilização pelas organizações, para avaliar e melhorar o próprio gerenciamento de riscos.

Como consequência, em 2004, foi publicado modelo ***Enterprise Risk Management – Integrated Framework*** (Gerenciamento de Riscos Corporativos – Estrutura Integrada), também conhecida como **Coso ERM** ou **Coso II**, que intensificou a preocupação com os riscos.

O prefácio da edição brasileira do novo modelo afirma que o Coso I tornou-se referência para ajudar empresas e outras organizações a avaliar e aperfeiçoar os sistemas de controle interno, sendo que essa estrutura foi incorporada em políticas, normas e regulamentos adotados por milhares de organizações com a finalidade de controlar melhor suas atividades de forma a cumprir os objetivos estabelecidos. Contudo, era necessário dar mais enfoque ao gerenciamento de riscos, incluindo os riscos relacionados aos objetivos estratégicos, que são os que dão suporte à sobrevivência da organização, razão por que o Coso II adicionou essa categoria de objetivo (estratégico) às três anteriormente estabelecidas pelo Coso I (operacional, comunicação e conformidade).

O Coso II, ao preconizar que a estrutura de gerenciamento de riscos abrange o controle interno, dá origem a uma conceituação mais robusta para assegurar o alcance de objetivos organizacionais, incluindo os objetivos relacionados à sobrevivência, à continuidade e à sustentabilidade das organizações (objetivos estratégicos).

Evoluiu-se, assim, da gestão centrada em controles funcionais para o desenvolvimento de uma cultura de risco, na qual todos os funcionários tornam-se responsáveis pela gestão de riscos e adquirem consciência dos objetivos do controle interno.

A atenção volta-se primeiramente para identificação dos riscos que possam impactar os objetivos da organização nas quatro categorias definidas pelo modelo para, em seguida, avaliar a forma como os gestores atuam para minimizar esses riscos, por meio de controles internos e de outras respostas.

O modelo Coso II será a base de desenvolvimento deste curso. O seu detalhamento será feito a partir do tópico 2, desta aula, quando trataremos dos elementos de um controle interno eficaz, integrando uma abordagem de gestão de riscos incorporada no referido modelo.

A nossa escolha pelo modelo Coso II está em consonância com a orientação da Intosai, que preconiza padrões de estruturas e processos de controle interno calcados no gerenciamento de riscos e em modelos de governança corporativa (INTOSAI GOV 9100, de 2004, atualizada pela INTOSAI GOV 9130, de 2007).

1.3 Outros modelos e regulamentações

Além dos modelos Coso I e II, existem ainda modelos e regulamentações aplicáveis a determinados segmentos específicos, dos quais destacamos os que se seguem.

COBIT e ITIL

Muitas organizações, atualmente, têm uma dependência crítica dos processos suportados por tecnologia da informação (TI). A informação e a tecnologia que a suporta passaram a constituir um ativo valioso, exigindo um adequado gerenciamento dos riscos relacionados e uma crescente necessidade de controle sobre as informações, fatores hoje considerados como elementos-chave da governança corporativa.

É nesse contexto que os modelos CobiT e Itil assumem importância fundamental como referências para a implementação de gerenciamento de riscos e avaliação de controles internos na área de TI.

O CobiT (*Control Objectives for Information and related Technology*), atualmente na versão 4.1, é um modelo formulado como *framework* para

governança e controle de TI pela Associação de Auditoria e Controle de Sistemas de Informação (Isaca, www.isaca.org), cuja manutenção e desenvolvimento (a versão 5 será lançada em 2012) são atualmente conduzidas pelo *IT Governance Institute* (www.itgi.org). O modelo, que se adéqua e dá suporte ao Coso, inclui sumário executivo, controle de objetivos, mapas de auditoria, ferramentas para implementação e, principalmente, um guia com técnicas de gerenciamento de riscos e governança na área de TI.

Informações mais completas e atualizadas sobre o CobiT e os produtos a ele relacionados, incluindo ferramentas *on-line*, guias de implementação, estudos de caso, notícias e material educacional, estão disponíveis no site www.isaca.org/cobit.

A Itil (*Information Technology Infrastructure Library*) constitui um conjunto de boas práticas aplicáveis à infraestrutura, operação e manutenção de serviços de TI, que busca promover a gestão com foco no cliente e na qualidade dos serviços de TI, caracterizando-se, assim, como um grande aparato ou modelo de "melhores práticas" utilizadas pelos gestores de TI, com o objetivo de fazer com que a área de TI foque no negócio da organização e entregue os seus serviços a seus clientes da melhor maneira possível e a um custo justificável.

Segundo Fernandes e Abreu (2008, p. 273), a biblioteca foi desenvolvida no final dos anos 80 pela CCTA (*Central Computer and Telecommunications Agency*), a partir de uma encomenda do governo britânico, que não estava satisfeito com o nível de qualidade dos serviços de TI a ele prestados. Atualmente na versão 3, conhecida como Itil V3, é mantida pelo OCG (*Office for Government Commerce*,organização do governo do Reino Unido responsável por iniciativas que aumentam a eficiência e efetividade de processos de negócio do governo).

Tanto CobiT como Itil são modelos de melhores práticas que podem ser aplicados a qualquer organização, pública ou privada, em conjunto com o Coso, obtendo-se, assim, um sistema de controle interno robusto, que abarca todas as atividades organizacionais, incluindo as executadas com suporte de TI.

Acordos de Basiléia e Normas do CMN

Os Acordos de Basiléia I, de 1988, e II, de 2001, elaborados no âmbito do *Bank for International Settlements* (BIS), tiveram por objetivo assegurar solidez e estabilidade ao sistema financeiro por meio de

controles de riscos, aliando atuação da supervisão bancária e maior transparência como formas eficientes para evitar o risco sistêmico.

Com base nesses acordos, o Conselho Monetário Nacional (CMN) determinou às instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil:

- Implantar e implementar controles internos voltados para as atividades por elas desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais (Resolução CMN n.º 2.554/1998).

- Implementar estrutura de gerenciamento do risco operacional (Resolução CMN n.º 3.380/2006).

- Implementar estrutura de gerenciamento do risco de crédito (Resolução CMN n.º 3.721/2009).

Essas normas são obrigatórias para as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, incluindo os bancos estatais, como por exemplo, Banco do Brasil e Caixa Econômica Federal.

Lei Sarbanes-Oxley

Promulgada nos Estados Unidos em 2002, na esteira de diversos escândalos corporativos, com o intuito de restabelecer a confiança da sociedade nas empresas de capital aberto (as que têm ações negociadas em bolsas de valores), a lei Sarbanes-Oxley (SOX) é considerada uma das mais rigorosas regulamentações a tratar de controles internos, elaboração de relatórios financeiros e divulgações.

As seções 302 e 404 têm sido o foco das atenções dos profissionais de auditoria por serem as que mais dizem respeito ao sistema de controle interno e às boas práticas de governança corporativa.

A seção 302, "*Corporate Responsability for Financial Reports*" (Responsabilidade Corporativa por Relatórios Financeiros), também conhecida como "certificações", exige que o principal executivo e o diretor financeiro assumam a responsabilidade pelas informações divulgadas nos relatórios financeiros, declarando, pessoalmente, que executaram a avaliação do desenho e da eficácia dos controles internos.

A seção 404, intitulada "*Management Assessment of Internal Control*" (Avaliação dos Controles Internos pela Administração), prescreve que

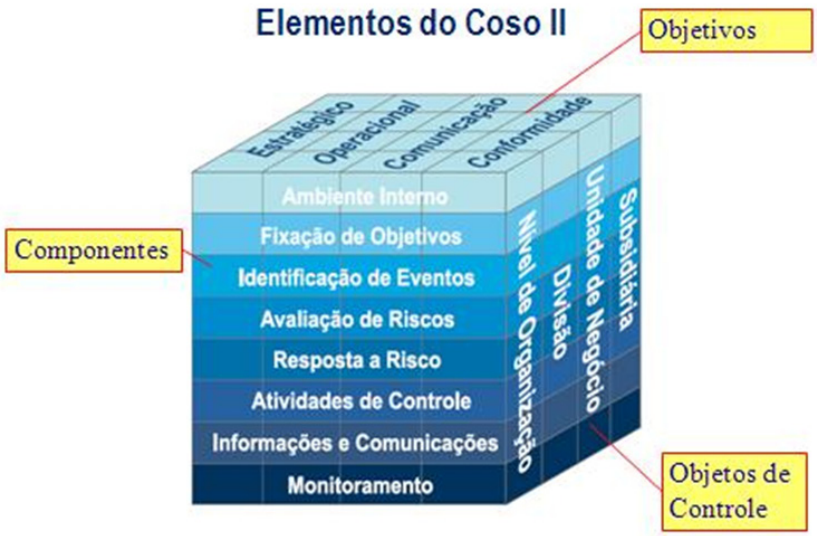
a alta administração da companhia é responsável pela adequação dos controles internos e exige que o principal executivo e o diretor financeiro avaliem e atestem, periodicamente, a sua eficácia. Além disso, exige a emissão, por auditoria independente, de um relatório distinto atestando a participação da administração nos estudos e na certificação da eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros.

As regras da SOX são obrigatórias para as empresas estrangeiras que possuam ações (ADR) negociadas no mercado norte-americano (EUA). É o caso, por exemplo, de Petrobrás, Vale, Eletrobrás, Itaú Unibanco, Bradesco, dentre tantas outras empresas brasileiras que lá negociam suas ações.

2. Elementos de um sistema de controle interno eficaz

O modelo Coso II traz, no formato de uma matriz tridimensional (ilustração abaixo, conhecida como Cubo Coso II), os elementos que devem constituir um sistema de controle interno considerado eficaz, apoiado numa estrutura de gerenciamento de riscos. Logo a seguir, cada um desses elementos será definido e terá o significado explicado, segundo a concepção do modelo.

Como já mencionado, o Coso II ampliou o alcance dos controles internos, oferecendo um enfoque mais vigoroso e extensivo ao tema, ao integrar técnicas de gerenciamento de riscos, sem abandonar, mas incorporando o Coso I. A nova postura defendida pelo modelo é que o controle interno deve integrar a gestão de riscos de modo a prever e a prevenir os riscos inerentes ao conjunto de processos da organização, que possam impedir ou dificultar o alcance de seus objetivos.



2.1 Objetivos

Embora muitos objetivos sejam específicos a uma determinada organização, o modelo definiu quatro **categorias de objetivos** comuns a praticamente todas as organizações (face superior do cubo), os quais devem ser previamente fixados (componente Fixação de Objetivos) para permitir a identificação (componente Identificação de Eventos) e análise dos riscos (componente Avaliação de Riscos) que poderão impactá-los, formando uma base de conhecimento para definir como esses riscos deverão ser gerenciados (componente Resposta a Riscos). Essas categorias de objetivo são as seguintes:

Estratégico: relacionado à sobrevivência, continuidade e sustentabilidade da organização. Referem-se às metas de alto-nível, alinhadas e servindo de suporte à missão.

Operacional: efetividade e eficiência das operações e adequada salvaguarda de ativos e recursos contra perdas, mau uso ou dano.

Comunicação: confiabilidade da informação produzida e sua disponibilidade para dar suporte ao processo decisório e para o cumprimento das obrigações de accountability.

Conformidade: aderência às leis e regulamentações aplicáveis à entidade, e às normas, políticas, aos planos e procedimentos da própria organização.

Interessante notar que as *Diretrizes para as Normas de Controle Interno do Setor Público* (INTOSAI, 2004) criaram uma categoria de objetivos adicional, denominada "***salvaguarda de recursos***", enquanto o Coso considera esse objetivo dentro da categoria operacional. Segundo a Intosai (2004, p.11), embora essa categoria possa ser vista como uma subcategoria do operacional, ela precisa, no caso do setor público, de cuidado especial e, portanto, precisa ser fortalecida.

A relação entre objetivos, riscos e controles, pode ser vislumbrada da seguinte maneira: tendo por base a missão e a visão da organização, a administração estabelece os planos principais nos quais fixa os objetivos, seleciona estratégias para alcançá-los e determina o alinhamento em todos os níveis da organização. Os riscos associados são identificados, avaliados e têm suas respostas definidas. Os controles de riscos que se mostrarem necessários devem ser então estabelecidos por meio de uma estrutura de gerenciamento de riscos e de controles internos, em todos

os níveis da organização, para fornecer uma razoável segurança de que os objetivos fixados serão alcançados.

Note-se que os objetivos de comunicação e de conformidade são controláveis, isto é, a organização tem ou deveria ter efetivo controle sobre eles, sendo esperado, portanto, que o controle interno ofereça uma garantia razoável em relação ao atendimento dos objetivos estabelecidos sob essas duas categorias.

O mesmo não ocorre em relação aos objetivos de natureza estratégica e operacional, já que a realização desses está sujeita à ação de eventos externos nem sempre sob controle da organização. Assim, é esperado que o controle interno seja capaz de propiciar uma garantia razoável de que a alta administração, na função de supervisão, será informada, no momento adequado, o quanto a organização está avançando no cumprimento dos objetivos estabelecidos sob essas duas categorias. É a visão do controle interno como base informativa para o processo decisório.

Outro aspecto a ser notado nessa categorização de objetivos é que ela não é estanque. Apesar de distintas, elas se inter-relacionam. Determinado objetivo pode ser classificado em mais de uma categoria, representar diferentes necessidades da organização e estar sob a responsabilidade direta de diferentes executivos. A classificação, contudo, é importante por permitir diferenciar o que pode ser esperado em cada categoria e melhor identificar os riscos a elas associados.

2.2 Objetos

A face lateral do cubo representa os níveis ou áreas da organização que são objeto da gestão de riscos e da incidência do controle interno. Observe-se que a visão integrada dos elementos do modelo demonstra o contexto das ações da administração ao gerenciar riscos e estabelecer controles na organização, em nível da entidade como um todo ou em nível da cada parte que a compõe. Assim temos:

- objetivos, riscos e controles em nível da organização ou de partes dela (divisão, unidade de negócio, departamento, projeto, seção etc.);

- objetivos, riscos e controles em nível de atividades (macroprocessos, processos, subprocessos, operações, sistemas ou atividades dentro desses).

2.3 Componentes

A face frontal da estrutura representa os componentes do gerenciamento de riscos, incorporando o sistema de controle interno, ou seja, aquilo que é necessário prover (os meios) para atingir os objetivos estabelecidos nas categorias da face superior do cubo. O modelo é composto de oito componentes inter-relacionados, por meio dos quais uma organização gerencia os riscos de maneira integrada ao processo de gestão.

Importante notar que para avaliar o sistema de controle interno de uma organização é necessário avaliar a presença e o funcionamento de cada um dos componentes da estrutura, quais sejam:

- Ambiente de controle (no Coso II, Ambiente interno)
- Avaliação de risco
- Atividades de controle
- Informação e comunicação
- Monitoramento

Note, ainda, que aos elementos acima, do Coso I, o Coso II acrescentou os seguintes, de maneira a permitir uma abordagem mais consistente do gerenciamento de riscos:

- Fixação de objetivos
- Identificação de eventos
- Resposta a risco

O estudo e o entendimento do detalhamento desses componentes são de importância fundamental para quem vai realizar trabalhos de avaliação, pois eles constituem a base dos critérios de avaliação de estruturas de gestão de riscos e controle interno em nível de entidade e para a implementação e avaliação de controles em nível de atividades, processos ou operações específicos.

Explicaremos cada um desses componentes a seguir.

Para um maior aprofundamento, recomendamos a leitura dos documentos "Gerenciamento de Riscos Corporativos – Estrutura Integrada", do Coso, "Diretrizes para as Normas de Controle Interno do Setor Público, da Intosai, e "Ferramenta de Gestão e Avaliação de Controle Interno", do GAO, disponíveis na biblioteca do curso.

2.3.1. Ambiente interno

O ambiente interno é um dos mais importantes componentes da estrutura. Ele é a base, o alicerce para todos os outros componentes da gestão de riscos e do sistema de controle interno, provendo disciplina e estrutura e proporcionando a atmosfera na qual as pessoas conduzem cotidianamente suas atividades e executam suas responsabilidades.

O ambiente interno é moldado pela história e cultura da organização e, por sua vez, molda, de maneira explícita ou não, a maneira como os negócios nela são conduzidos. É o que chamamos de tom da organização, refletindo a cultura de riscos e a forma como eles são encarados e gerenciados, influenciando a consciência de controle das pessoas.

Os fatores que compõem o ambiente interno incluem integridade e valores éticos, competência das pessoas, "perfil dos superiores" (ou seja, a filosofia da direção e o estilo gerencial: "*o exemplo vem de cima*."), estrutura organizacional e de governança, atribuição de autoridade e responsabilidade, políticas e práticas de recursos humanos.

Vejamos, em síntese, o significado dos principais fatores que compõem o ambiente interno.

Integridade e Valores Éticos

Todas as pessoas, desde o mais alto dirigente ao funcionário de menor hierarquia, devem ser estimuladas a agir com integridade e ética. A alta administração deve dar exemplo e enfatizar a todos o que deles é esperado em termos de integridade e valores éticos. Códigos de conduta devem ser formalizados e comunicados a todos dentro da organização. Ações disciplinares para não conformidades devem ser estabelecidas, comunicadas e gerenciadas consistentemente.

A alta administração, na busca do estabelecimento de padrões de integridade e valores éticos, deve procurar alcançar equilíbrio entre os interesses da organização, de seus empregados, fornecedores, clientes e do público em geral, minimizando os conflitos potenciais e desestimulando práticas fraudulentas e ilegais ou, no mínimo, pouco éticas.

Numa entidade em que a cultura organizacional não é calcada em princípios éticos e valores morais, a probabilidade de ocorrência de fraudes e outras irregularidades é, invariavelmente, alta. Ênfase em resultados de curto prazo, a qualquer custo, pode levar à prática de atos ilícitos ou antiéticos.

Nesse sentido, o chamado "tom do topo", ditado pela direção superior e gerência da organização, constitui um elemento crítico para um ambiente de controle interno saudável. As atitudes, as percepções e os valores éticos predominantes na cultura organizacional constituem o principal indicador de eficácia do sistema de controle interno como um todo.

A empresa norte-americana Enron, uma gigante do setor energético, sofreu a maior falência da história econômica americana devido a várias práticas contábeis e operacionais escusas relacionadas ao ambiente de controle interno (conflitos de interesse, pressão por metas, práticas de avaliação contábeis agressivas, auditoria e consultoria pelos mesmos auditores etc.).

Filosofia da direção e estilo gerencial

A filosofia da direção e o estilo gerencial adotados para conduzir os negócios da organização marcam o nível de risco em que esta opera, afetando o controle interno. Atitudes pouco prudentes na condução dos negócios e desconsideração de aspectos relacionados ao controle ou às boas práticas administrativas degeneram o ambiente interno, elevando os níveis de risco na organização.

Por outro lado, se ao empreender novos negócios, projetos ou mudanças relevantes, os riscos são cuidadosamente avaliados, considerando os aspectos positivos e negativos de cada alternativa, e só são aceitos após deliberação em instâncias adequadas, a mensagem que a administração transmite é de reforço a uma cultura de responsabilidade.

A direção superior, ao demonstrar o seu compromisso e a sua liderança, no que diz respeito aos controles internos, aos demais níveis da organização, apoiando a auditoria interna e outras áreas críticas para o controle, bem como os planos de ação recomendados pela auditoria interna e pelos órgãos de controle, transmite a mensagem que controle interno é importante e os demais membros da organização sentirão essa atitude e a responderão, observando conscientemente os controles estabelecidos.

Estrutura organizacional e de governança

A estrutura organizacional de uma entidade fornece a base para o planejamento, a execução, o controle e a correção de rumos de suas atividades. Envolve a determinação das principais áreas de autoridade e responsabilidade e as suas linhas de subordinação, juntamente com procedimentos efetivos para monitorar resultados (*accountability*).

Essa estrutura deve ser estabelecida de maneira a favorecer o cumprimento da missão e o alcance dos objetivos da organização, bem como a eficácia do gerenciamento de riscos e do controle interno. Tal estrutura é, geralmente, formalizada por meio de um organograma e complementada por um manual da organização ou instrumentos normativos (resoluções, portarias etc.) que estabelecem competências, atribuições e responsabilidades das unidades e dos cargos que as compõem.

Poderes delegados devem ser adequados para lograr as metas e os objetivos da organização, bem como para cumprir as funções operacionais e exigências regulatórias, e aqueles que os recebem devem conhecer corretamente suas responsabilidades e prestar contas de como as desincumbem. A segregação de funções incompatíveis, de extrema importância para o controle interno, deve ser levada em conta na concepção da estrutura, para prevenir que o desenho organizacional não favoreça a prática de ações indesejadas.

Estrutura organizacional e de governança adequadas devem ser compatíveis com o porte, as atividades e a complexidade dos interesses das partes envolvidas. Dependendo do porte da organização, uma robusta estrutura de governança pode ser necessária, o que pode incluir um conselho superior (por exemplo, conselho de administração), conselho fiscal, auditoria interna, comitê de auditoria e outros comitês ou comissões de assessoramento ou setoriais (de risco, de crédito, de coordenação geral, de gestão de pessoas etc.) para promover um adequado equilíbrio dos interesses de todas as partes interessadas.

O ambiente de controle interno é fortalecido pela presença desses instrumentos, todavia, apenas a sua existência formal não é suficiente. Sobretudo, é necessário que os membros da estrutura organizacional e da governança tenham adequada capacidade e elevado conhecimento e experiência em suas áreas, de maneira que suas atuações apoiem objetivamente a governança e o alcance dos objetivos da organização.

Políticas e práticas de Recursos Humanos

As pessoas constituem o mais valioso ativo de qualquer organização e, portanto, devem ser tratadas de maneira que se consolidem tecnicamente e como pessoa humana e, assim, possam ofertar o melhor rendimento para o alcance dos objetivos da organização.

Como já mencionado, controles internos são executados por pessoas e, dessa forma, a qualidade dos servidores da entidade afetam

diretamente o ambiente interno e, consequentemente, todos os outros componentes do sistema, em especial a execução dos controles.

Políticas e práticas para contratar, capacitar, orientar, avaliar, promover, recompensar, disciplinar e demitir funcionários devem ser estabelecidas e comunicadas de modo claro, sendo essa uma responsabilidade da administração nos seguintes momentos:

- **Seleção**: a organização deve estabelecer requisitos adequados de conhecimento, experiência (habilidades) e atitudes (integridade) para as contratações de seu pessoal.

- **Compromisso com a competência**: organizações com ambiente interno efetivo contratam e mantém pessoas competentes para desempenhar suas tarefas e exercer suas responsabilidades de maneira eficaz.

    - Toda organização deve ter procedimentos para identificar e definir as competências necessárias para o desempenho das funções e preenchimento dos cargos de maneira a poder selecionar, formar, avaliar e promover o seu pessoal, suprindo cada posto de trabalho com pessoas capazes de realizar suas tarefas de forma competente.

    - A organização deve estabelecer um programa de capacitação e insistir para que todos sejam adequadamente capacitados para desempenhar as funções de maneira proveitosa. Funcionários novos devem ser metodicamente familiarizados com a cultura e os procedimentos da organização e todos os empregados devem ter treinamento contínuo para bem desempenhar suas atividades.

- **Avaliação de desempenho**: deve ter critérios vinculados às metas e aos objetivos fixados no plano estratégico da organização e em seus desdobramentos. Os funcionários devem receber *feedback*, aconselhamento e sugestões de melhoria sobre seu desempenho.

- **Promoções, recompensas e rotatividade**: devem estar atreladas à avaliação de desempenho e ao nível de capacitação alcançado pelo servidor.

- **Sanção**: medidas disciplinares devem ser adotadas, quando cabíveis, para transmitir rigorosamente a ideia de que desvios não são tolerados.

2.3.2. Fixação de objetivos

Toda organização tem uma razão para existir, que é a sua missão, e, para lhe dar cumprimento é necessário que estabeleça objetivos e estratégias para alcançá-los.

Como todos os objetivos de uma organização envolvem, de certa maneira, uma parcela considerável de riscos, é necessário mitigá-los, identificando-os, avaliando-os e decidindo se devem ser modificados por algum controle. Assim, os objetivos devem ser definidos *a priori* para que seja possível identificar os riscos a eles associados.

Os termos **"resposta a riscos"** e "tratamento de riscos" são usados indistintamente ao longo deste curso.

A explicitação de objetivos, alinhados à missão e à visão da entidade, é necessária para permitir a identificação de eventos que tenham o potencial para impedir ou dificultar a sua consecução. Definir os objetivos é, pois, uma pré-condição para identificação de riscos e para avaliação e definição de estratégias para gerenciá-los (**resposta a riscos**).

O modelo Coso requer que todos os níveis da organização tenham objetivos fixados e comunicados, ou seja, no nível da organização como um todo e para todas as divisões, processos e atividades. Além disso, para cada objetivo, a organização deve estabelecer padrões de como eles devem e podem ser atingidos e como o seu grau de atingimento deve ser mensurado. Ou seja, objetivos devem ser comunicados juntamente com declarações de expectativas relativas ao grau ou nível de excelência ou, ainda, ao que é possível alcançar em termos de qualidade e desempenho desejado, incluindo indicadores que serão utilizados para monitorar o alcance desses padrões.

No setor público, muito embora os objetivos sejam relacionados com e originem-se de programas de governo ou sejam estabelecidos na legislação, o detalhamento desses objetivos, conforme exigido pelo modelo, é feito pela administração de cada entidade ou órgão público em seu planejamento estratégico. Em seguida, esses objetivos são desdobrados em ações e metas pela direção e gerência (nível tático) até chegar aos planos de ação ou de trabalho, no nível operacional da organização. Isso demonstra o quanto é imprescindível o planejamento estratégico nas organizações públicas, bem como o seu desdobramento em planos táticos e operacionais, programas e projetos, por todos os níveis organizacionais.

2.3.3. Identificação de eventos

Uma vez fixados os objetivos, devem-se identificar os eventos ou **riscos-chave** que ameacem o seu cumprimento. A identificação de eventos consiste em identificar a existência de situações que possam impedir ou a ausência de situações consideradas necessárias ao alcance dos objetivos-chave fixados, tanto em nível da organização como um todo como em cada nível significativo de suas atividades (unidades de negócio, operações e processos organizacionais).

O modelo Coso trata do conceito de **eventos potenciais**, definindo-os como um incidente ou uma série de incidentes resultantes de fatores internos ou externos, que possam afetar a implementação da estratégia e o alcance dos objetivos. **O processo de identificação de eventos pode abranger tanto os riscos negativos, tidos como ameaças, como os eventos positivos, vislumbrados como oportunidades**. Os primeiros, levando a organização a alcançar objetivos abaixo das expectativas, os segundos, levando a organização a alcançar resultados superiores aos obtidos atualmente ou além das expectativas.

Segundo a norma ISO NBR 31000/2009, a identificação de riscos é o processo de busca, reconhecimento e descrição de **eventos** e envolve a identificação das **fontes de risco**, das **causas** e das **consequências** potenciais dos eventos (ISO NBR 31000/2009, 2.15 e Nota 1).

Evento é a ocorrência ou alteração em um conjunto específico de circunstâncias e também pode consistir em alguma coisa não acontecer, bem como consistir em uma ou mais ocorrências e pode ter várias causas (ISO NBR 31000/2009, 2.17 e Notas 1 e 2).

Fonte de risco é o elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco, podendo ser tangível ou intangível (ISO NBR 31000/2009, 2.16 e Nota). São todos os sujeitos, objetos ou situações que têm o potencial para originar um evento. As fontes de risco são classificadas em seis categorias: pessoas, processos, sistemas, infraestrutura (física ou organizacional), tecnologia ou ainda eventos externos à organização.

A **causa** potencial de um evento é composta pela associação de vulnerabilidades (inexistência, inadequação, insuficiência) a uma fonte de risco (pessoas, processos, sistemas ou infraestrutura, tecnologia ou eventos externos). Assim, são exemplos de causas pessoas sem capacitação, processos mal concebidos, deficiências ou inexistência de controles internos, instalações inadequadas, obsolescência tecnológica etc.

A vulnerabilidade pode ser entendida como a condição que deixa uma fonte de risco suscetível a originar um evento.

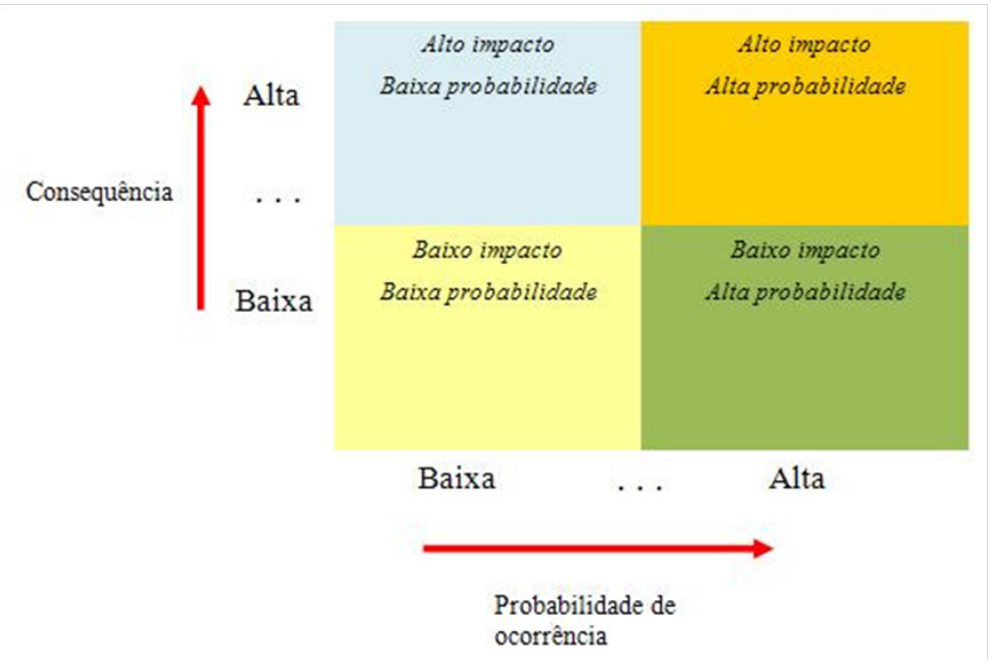
Consequência é o resultado de um evento que afeta os objetivos. Um mesmo evento pode levar a uma série de consequências, que podem ser expressas qualitativa ou quantitativamente e podem ter efeitos positivos ou negativos sobre os objetivos. Consequências iniciais podem desencadear reações em cadeia (ISO NBR 31000/2009, 2.18 e Notas 1 a 4).

Para a Intosai (2004, p. 23), a identificação de riscos deve ser um processo contínuo, repetitivo, muitas vezes integrado ao processo de planejamento, para identificar riscos relevantes relacionados aos objetivos-chave da organização, resultando em uma pequena quantidade de riscos-chave que serão considerados num enfoque estratégico para avaliação de risco. Isso é importante tanto para identificar as áreas/atividades mais relevantes, para as quais se devem dirigir esforços de avaliação dos riscos, como também para atribuir responsabilidades em relação ao seu gerenciamento.

2.3.4. Avaliação de riscos

Uma vez identificados, os riscos devem ser avaliados sob a perspectiva de probabilidade de sua ocorrência e consequências de sua materialização. O objetivo da avaliação é formar uma base para o desenvolvimento de estratégias para tratamento dos riscos identificados (resposta a risco), de maneira a diminuir a probabilidade de sua ocorrência e/ou a magnitude de suas consequências.

A ISO NBR 31000/2009 (2.23) conceitua **nível de risco** como a magnitude de um risco, ou combinação de riscos, expressa em termos da combinação de consequências e probabilidades. Um dos propósitos-chave da avaliação de risco é informar à administração sobre as áreas onde é necessário adotar uma ação (tratamento/resposta a risco) e qual o seu grau de prioridade (INTOSAI, 2004, p.24-25). Isso exige que se desenvolva um enquadramento para estabelecer níveis de riscos, por exemplo – em alto, médio ou baixo – como ilustrado na matriz seguinte, indicada pela Intosai (2007, p.28):



Fonte: Further Information on Entity Risk Management, Intosai, 2007, p. 28 (com adaptações)

A avaliação de riscos pode ser feita por meio de análises qualitativas e quantitativas, ou da combinação de ambas. Os gestores são responsáveis pela avaliação dos riscos no âmbito das unidades de negócio, de processos e atividades que lhes são afetos. A alta administração deve avaliar os riscos no nível da organização, desenvolvendo uma visão de riscos de forma consolidada (perfil de risco). Riscos devem ser avaliados quanto à condição de inerentes e residuais.

2.3.5. Resposta a Riscos

É o processo de desenvolver e determinar estratégias para gerenciar os riscos identificados. O modelo Coso II identifica quatro categorias de resposta a riscos: **evitar**, **reduzir**, **compartilhar** e **aceitar**, cuja escolha dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco. Isto quer dizer que compete à administração obter uma visão dos riscos em toda organização e desenvolver um conjunto de ações concretas, abrangendo essas quatro categorias de respostas, para manter o nível de riscos residuais alinhado aos níveis de tolerância e apetite a riscos estabelecidos pela organização.

A Intosai, no documento INTOSAI GOV 9130, refere-se às categorias de resposta a riscos como: evitar/encerrar a atividade, reduzir/tratar, compartilhar/transferir e aceitar/tolerar. A norma de gestão de riscos ISO ABNT 31000/2009 engloba sob o título "tratamento de riscos" todos os tipos possíveis de resposta a riscos.

Conforme a INTOSAI GOV 9100/2004 (p. 25 e 69), apetite a risco é a quantidade de risco que uma organização está propensa a se expor para alcançar seus objetivos. Reflete a cultura gerencial ou a predisposição – cautelosa ou agressiva – a respeito de assumir riscos na perseguição da missão ou visão da entidade. A tolerância a riscos é a variação aceitável relativa à realização de um objetivo específico. É uma derivação tolerável

do nível de apetite a risco definido e dos objetivos organizacionais (exemplo: projetos devem ser concluídos no prazo e dentro do orçamento estipulado, mas uma variação de até 15% no prazo e de até 10% no custo total é tolerada). A determinação de respostas a riscos deve levar em consideração essas duas variáveis.

O tipo de resposta a ser adotado, dentre as quatro categorias possíveis tratadas a seguir, é uma consequência da avaliação que se fez do risco em confronto com o apetite e a tolerância da entidade ao risco.

Evitar (ou, ainda, **encerrar** a atividade, segundo a Intosai): é a decisão de não iniciar ou de descontinuar a atividade sujeita ao risco.

Reduzir (ou também **tratar**, segundo a Intosai): é a adoção de medidas para reduzir a probabilidade ou a consequência dos riscos ou até mesmo ambos. Na maior parte dos casos, o risco deverá ser tratado, gerando a necessidade de implementar e manter um efetivo sistema de controle interno. Os procedimentos que uma organização estabelece para tratar riscos são denominados atividades de controle (INTOSAI, 2004, p. 26), componente que será estudado no próximo tópico.

Compartilhar (ou também **transferir**, segundo a Intosai): é mitigar a consequência e/ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco, mediante contratação de seguros, operações de *headging* ou terceirização de atividades nas quais a organização não tem *expertise*.

Aceitar (ou também **tolerar**, segundo a Intosai): é não tomar, deliberadamente, nenhuma medida para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização ou a capacidade para fazer qualquer coisa sobre o risco é limitada ou, ainda, o custo de tomar qualquer medida é desproporcional em relação ao benefício potencial.

Resumindo, **Evitar** é descontinuar ou não iniciar algo porque nenhuma outra opção de resposta foi considerada suficiente para reduzir a probabilidade e/ou a consequência de maneira que o risco residual ficasse dentro do nível de tolerância considerado aceitável pela organização. **Reduzir** ou **Compartilhar** são opções de resposta que reduzem o risco residual a um nível de compatibilidade com a tolerância a risco da organização, enquanto **Aceitar** indica que o risco inerente já está dentro do nível de tolerância, ou porque a capacidade para fazer alguma coisa em relação ao risco é limitada por algum fator, ou pelo custo/benefício.

Ao determinar respostas a riscos, a administração deverá levar em consideração:

- os efeitos das respostas estudadas sobre a probabilidade e a consequência dos riscos e a compatibilidade das respostas com as tolerâncias a risco da organização;
- os custos versus os benefícios das respostas em estudo;
- as possíveis oportunidades contidas nas opções de resposta, que podem levar a organização a alcançar objetivos além do permitido, e não só pela redução dos riscos.

Vejamos o que significa cada uma destas considerações.

Avaliação dos efeitos das respostas estudadas sobre a probabilidade e a consequência dos riscos

Na avaliação das opções de resposta é necessário levar em conta que determinadas respostas podem afetar, de forma diferente, a probabilidade e a consequência do risco. Às vezes a consequência de um evento pode não mudar com a adoção de determinada resposta, mas a probabilidade dele acontecer é reduzida. Noutras vezes, a solução pode não reduzir a probabilidade, mas circunstâncias específicas podem atenuar o impacto da consequência do evento mitigado.

Avaliação de custos versus benefícios das respostas

É necessário considerar os custos e os benefícios relativos às opções de respostas alternativas ao risco. Embora muitas vezes seja difícil quantificar os custos de resposta a riscos e mais ainda os benefícios, pelos menos os custos diretos precisam ser considerados. Benefícios de programas de treinamento, por exemplo, geralmente são aparentes, mas difíceis de quantificar. Em casos como esses, o benefício da resposta pode ser avaliado no contexto do benefício associado com a realização do objetivo correspondente.

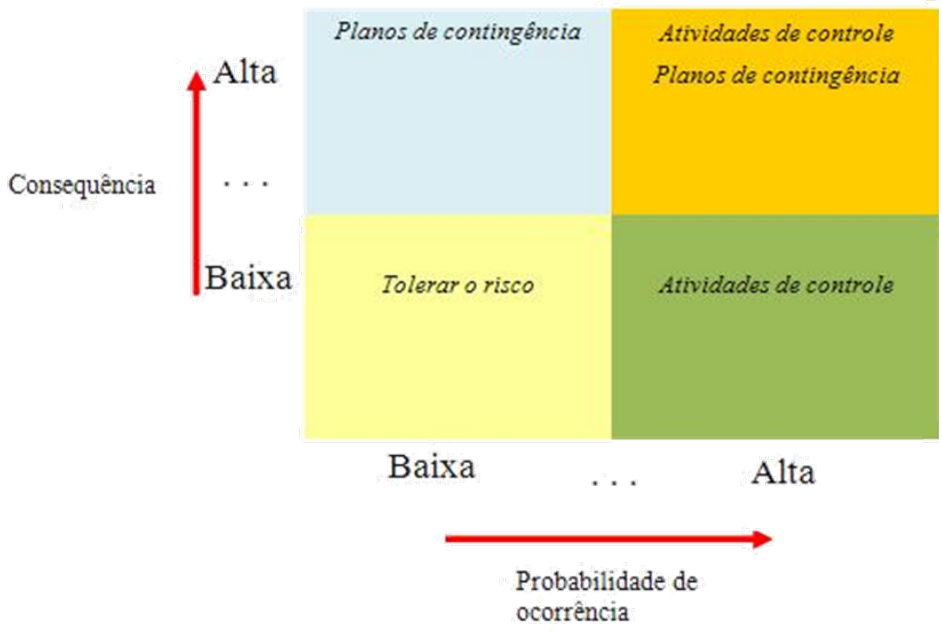
No caso de a organização decidir pela opção de reduzir ou tratar um risco, a avaliação de custo-benefício da atividade de controle planejada é muito importante para o gestor tomar a decisão de instituí-la. Se o dano causado pela ocorrência do evento for menor do que o custo de controle, ou menor do que a opção de transferir o risco, o melhor para a administração será aceitar o risco. Em todos os casos, a avaliação da tolerância ao risco deve ser levada em consideração pela administração na decisão sobre a resposta ao risco.

Avaliação das oportunidades nas opções de respostas

Ao avaliar opções de respostas, a administração deve adotar uma visão abrangente em relação ao que é possível fazer, além de tão somente focar em soluções diretas para lidar com o risco específico. Ou seja, considerações de respostas a riscos não devem se limitar exclusivamente à redução direta dos riscos, mas incorporar uma visão de prospecção de novas oportunidades para a organização.

Ao adotar essa postura, é possível identificar oportunidades durante o estudo das opções de resposta ao risco, que, se implementadas, trarão benefícios além daqueles proporcionados pela simples atuação direta para a redução de um risco específico. Tais oportunidades podem representar respostas inovadoras e normalmente emergem quando as opções de resposta a riscos atingem o limite da eficácia. O Coso cita o exemplo de uma resposta criativa de uma companhia de seguros de automóveis ao elevado número de acidentes em certos cruzamentos. Essa companhia decidiu financiar melhorias nos semáforos existentes, fato que reduziu os sinistros e melhorou suas margens operacionais.

Para auxiliar o processo de seleção de respostas a riscos, a organização pode desenvolver uma matriz na qual as respostas potenciais estão associadas aos níveis de risco avaliados, conforme a sugestão a seguir da Intosai.



Fonte: Further Information on Entity Risk Management, Intosai, 2007, p. 28 (com adaptações)

Uma vez escolhida uma resposta, a administração poderá necessitar desenvolver um plano de implementação para executá-la. Uma parte crítica desse plano é o estabelecimento de atividades de controle (estudadas no componente a seguir) para assegurar-se de que as respostas aos riscos determinadas pela administração sejam efetivamente executadas.

2.3.6. Atividades de controle

As atividades de controle são assim denominadas pelo Coso e pela Intosai. Entre nós elas são mais conhecidas simplesmente como **"controles internos"**.

Ao selecionar respostas a riscos, a administração deve identificar as atividades de controle necessárias para assegurar que tais respostas sejam executadas de forma adequada e oportuna. Ou seja, após o processo de fixação de objetivos e padrões para seu alcance, e após a identificação e avaliação dos eventos em potencial (riscos) que podem impactá-los, bem como da definição de respostas para enfrentá-los, a administração deve assegurar que tais respostas sejam efetivamente executadas, e, para isso, estabelece atividades de controle.

> As atividades de controle consistem em políticas e procedimentos estabelecidos, e de fato executados, para atuar sobre os riscos e contribuir para que os objetivos da organização sejam alcançados dentro dos padrões estabelecidos.
>
> O propósito fundamental das atividades de controle é reforçar a realização dos planos traçados, mantendo as organizações direcionadas para o cumprimento dos objetivos estabelecidos. Assim, elas podem ser vistas como mecanismos de gestão do cumprimento de objetivos.

As atividades de controle são parte do sistema de controle interno e, mesmo numa perspectiva do conjunto de todas elas, não devem ser confundidas com o ele próprio. Elas são um dos cinco componentes do sistema, quando baseado no modelo Coso I, ou dos oito, quando integra a gestão de riscos, no modelo Coso II.

Para uma revisão do conceito e da função de **controles preventivos e detectivos**, leia o tópico 1.5.1, da Aula 1.

De modo geral, as atividades de controle incluem dois elementos: uma política, que estabelece aquilo que deverá ser feito e os procedimentos para fazê-la ser cumprida. O grau de formalização varia entre as entidades, conforme o tamanho, a complexidade e o número de níveis hierárquicos, embora os conceitos subjacentes não se diferenciem de maneira significativa. Elas devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções, conforme requeridas pelas decisões de resposta a riscos. Elas incluem uma gama de **controles preventivos e detectivos**, como os exemplificados a seguir:

- atribuição de autoridade e limites de alçada;
- procedimentos de autorização e aprovação;
- segregação de funções ou atividades;
- rotatividade de funções
- revisões independentes, verificações e conciliações;
- avaliações de desempenho operacional;
- avaliações de operações, processos e atividades;
- supervisão direta;
- controles de acesso a recursos e registros.

Algumas atividades de controle nem sempre são pertinentes em pequenas organizações, nas quais canais de comunicação envolvem poucas camadas e existe uma estreita interação das pessoas e uma supervisão aplicada diretamente pela gerência de maneira eficaz. As principais atividades de controle e as respectivas classificações por função (prevenção ou detecção) são explicadas a seguir.

Atribuição de autoridade e limites de alçada (Prevenção)

Consiste em estabelecer competências e limites, de acordo com a posição hierárquica de órgãos e unidades da estrutura organizacional e de governança ou as responsabilidades gerenciais de ocupantes de cargos e funções, quanto à possibilidade de autorizar, executar ou aprovar atos ou transações em nome da organização. É uma forma de assegurar que os atos administrativos sejam realizados por quem tem o respaldo da organização para efetivá-los.

Procedimentos de autorização e aprovação (Prevenção/ Detecção)

Esse tipo de atividade, muitas vezes, tem conexão com a anterior. Uma vez fixados os limites de alçada e as competências para exercê-los, a administração determina quais atividades ou transações necessitam de uma autorização e aprovação superior para que sejam efetivadas.

A finalidade da autorização é assegurar que apenas os atos administrativos os quais a administração tem intenção de realizar

sejam iniciados. A aprovação, de forma manual ou eletrônica, implica a validação do ato e certificação da conformidade com as políticas e os procedimentos estabelecidos pela organização.

Salvo nos casos de aprovação prévia de propostas (solicitações, pedidos, requisições, por exemplo), a aprovação é um procedimento posterior à realização de atos anteriormente autorizados. Os responsáveis pela aprovação normalmente verificam a documentação pertinente, questionam itens e asseguram-se de que os preceitos necessários à conformidade do ato estão checados, antes de darem a sua aprovação.

As políticas que instruem os procedimentos de autorização e aprovação devem ser formalmente estabelecidas e comunicadas a todos os gestores e funcionários e incluir as condições específicas e os termos segundo os quais eles devem ser realizados. Por sua vez, os procedimentos de autorização e aprovação devem ser formalizados e documentados nos processos ou sistemas onde ocorrerem.

Segregação de funções ou atividades (Prevenção)

A segregação de funções ou atividades é um princípio básico de controle interno essencial para a sua efetividade. Consiste na separação de atribuições ou responsabilidades entre diferentes pessoas em funções ou atividades-chave de autorização, execução, registro, custódia e revisão/atesto/aprovação ou auditoria.

Boynton et al. (2002, p.331) traz uma excelente definição para segregação de funções:

> Segregação de funções envolve fazer com que indivíduos não realizem funções incompatíveis. [...] funções são consideradas incompatíveis quando é possível que um indivíduo cometa um erro ou fraude e esteja em posição que lhe permita esconder o erro ou a fraude no curso normal de suas atribuições.

A segregação de funções reduz o risco de erros humanos e de ações indesejadas e o risco de não detectar tais ocorrências, muito embora o conluio entre pessoas possa reduzir ou destruir a eficácia desta atividade de controle.

Exemplificando: quem é responsável pela guarda ou custódia de recursos financeiros não deve ser a mesma pessoa que tem poder para autorizar a movimentação desses recursos nem de registrar tais movimentos. Seguem-se outros exemplos de funções ou atividades que

deveriam ser segregadas para evitar o exercício, por uma mesma pessoa, de funções incompatíveis.

Exemplo 1: funcionário é responsável por receber no caixa valores decorrentes de vendas e registrar na contabilidade.

Risco de fraude: ficar com o dinheiro, omitindo registros de recebimentos; registrar devoluções de vendas ou não baixar contas recebidas.

Conclusão: quem processa recebimentos de caixa (execução e custódia) não deve ter atribuição de fazer o lançamento contábil da transação (registro).

Exemplo 2: funcionário é o responsável pela compra, recebimento, guarda e controle de materiais.

Risco de fraude: ficar com parte do material ou receber em quantidade menor que a efetivamente adquirida, omitindo a subtração nos registros documentais.

Conclusão: quem compra e recebe materiais (execução) não deve ser responsável pela guarda (custódia) e controle (registro).

Organizações de pequeno porte, com poucos funcionários, podem ter dificuldades para implementar essa atividade de controle, no entanto, devem estar consciente dos riscos e compensá-la com outros controles, como revisão independente de atividades (é o caso da adoção de controles compensatórios, cujo conceito foi estudado na Aula 1).

Rotatividade de pessoas em funções (Prevenção)

A rotatividade de pessoas em funções significa impedir que a mesma pessoa seja responsável por atividades sensíveis por um longo período de tempo. Tem uma finalidade semelhante à segregação de funções, impedir que uma pessoa cometa um erro ou fraude e possa esconder a situação por muito tempo. A exigência de gozo de férias anuais tem o efeito de rotatividade temporária de funções.

Revisões independentes, verificações e conciliações (Detecção)

As **revisões independentes** consistem na revisão de atos ou transações por um terceiro, não envolvido na sua execução. Esse tipo de atividade de controle é muitas vezes utilizado para compensar a não adoção de outros controles preventivos ou detectivos, ou para

contrabalançar outras falhas na estrutura de controle da organização como, por exemplo, a ausência de segregação de funções. Quando isso ocorre, o controle é denominado compensatório, embora, na essência, seja um controle detectivo.

As **verificações** ou conferências são controles básicos em qualquer atividade. De acordo com a Intosai (2004, p.30):

> As transações e os eventos significativos devem ser verificados antes e depois de ocorrerem, por exemplo: quando os produtos são entregues, o número de produtos entregues é conferido com o número de produtos solicitados. Depois, o número de produtos faturados é verificado com o número de produtos recebidos. O inventário também é verificado quando se realizam os balanços no almoxarifado.

As **conciliações** são atividades de controle que consistem em confrontar registros com documentos apropriados como, por exemplo, registros patrimoniais com relatórios de inventários de bens, registros contábeis de contas bancárias com extratos bancários correspondentes etc. Para serem efetivos, os procedimentos de conciliação devem ser periódicos e realizados com regularidade.

Vejamos um exemplo muito comum de conciliação – a conciliação bancária – utilizada para detectar lançamentos indevidos, erros ou fraudes, tanto por parte das instituições bancárias como por parte da contabilidade ou do controle financeiro da própria organização.

Conciliação Bancária

Contas	Extrato	Contabilidade	Diferença
Banco do Brasil	120,00	100,00	-20,00
Banco Real	150,00	150,00	-
Caixa Econômica	60,00	70,00	10,00

As diferenças encontradas numa conciliação devem ser devidamente explicadas, comprovadas e documentadas e os ajustes correspondentes, quando cabíveis, devem ser feitos nos registros e na contabilidade. As diferenças acima, por exemplo, poderiam gerar ou não ajustes contábeis ou nos controles financeiros da organização, conforme ilustrado a seguir:

Banco do Brasil – não gera lançamento de ajuste na contabilidade, pois se refere a cheque emitido e ainda não apresentado ao banco.

Caixa Econômica – gera lançamento de ajuste na contabilidade e no controle financeiro da conta corrente, pois se refere à despesa bancária de manutenção da conta, legitimamente debitada pela instituição, conforme lançamento no extrato bancário.

Observa-se, assim, que esse é um tipo de atividade de controle de grande importância para assegurar a confiabilidade dos registros que servem de base tanto para o processo decisório interno da organização como para o cumprimento das obrigações de *accountability*, ou seja, um dos objetivos do controle interno, conforme a Intosai e o Coso.

Avaliações de desempenho operacional (Detecção)

As avaliações de desempenho operacional permitem à administração verificar se os resultados obtidos estão alcançando os objetivos e padrões pré-estabelecidos. Quando isso não está ocorrendo, as operações, processos e atividades deverão ser objeto de avaliação (atividade de controle estudada a seguir) para determinar se é necessário implementar melhorias.

As avaliações de desempenho operacional incluem **revisões da alta direção**, ao comparar o desempenho atual em relação ao orçado, às previsões, aos períodos anteriores e aos concorrentes, bem como a análise crítica de **indicadores de desempenho**, relacionando-se diferentes conjuntos de dados, sejam eles operacionais ou financeiros, em conjunto com a realização de análises dos relacionamentos e das medidas de investigação e correção.

Indicadores de desempenho incluem, por exemplo, índices de rotação, de processos instruídos por unidade/por servidor etc., que conjugados com a investigação de resultados inesperados ou tendências incomuns permitirão à administração identificar circunstâncias nas quais a falta de capacidade para concluir processos fundamentais pode significar menor probabilidade de objetivos estabelecidos serem alcançados (COSO II, p.61).

Avaliações de operações, processos e atividades (Detecção)

Consiste no aprofundamento de investigações resultantes de avaliações de desempenho operacional ou em avaliações periódicas para assegurar que operações, processos e atividades cumprem com regulamentos, políticas, procedimentos ou outros requisitos em vigor.

Importante frisar que esse tipo de avaliação deve ser claramente distinto do monitoramento do controle interno, que será o último componente a ser estudado neste tópico do curso.

Supervisão direta (Prevenção/Detecção)

A supervisão direta, presente em todos os níveis da organização, consiste no acompanhamento do trabalho delegado aos funcionários pelo respectivo superior hierárquico. Inclui atividades de comunicação de atribuições, revisão e aprovação de trabalhos, bem como de orientação e treinamento do pessoal supervisionado para o desempenho das atribuições.

Para a Intosai (2004, p.31), a supervisão compreende:

- comunicação clara das funções e responsabilidades atribuídas a cada membro da equipe e da obrigação de prestar contas;
- revisão sistemática do trabalho de cada membro na extensão necessária;
- aprovação do trabalho nas etapas críticas para assegurar que flui como pretendido.

Ademais, a supervisão deve fornecer aos funcionários a orientação e o treinamento necessários para ajudar a assegurar que erros, desperdícios e atos ilícitos sejam minimizados e que as diretrizes gerenciais sejam compreendidas e cumpridas.

Controles de acesso a recursos e registros (Prevenção)

Os ativos críticos da organização devem ser protegidos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida. Assim, a depender do risco percebido em relação a essas ocorrências, deve-se estabelecer controles para limitar o acesso a recursos e registros (computadores, estoques, títulos, dinheiro, registros, bens etc.) às pessoas autorizadas a sua guarda, conservação e controle, as quais devem ser obrigadas a prestar contas de sua custódia e utilização. Incluem-se dentre essas atividades, os controles físicos e lógicos de acesso (controles de entrada/saída de pessoas, veículos, bens e materiais; criptografia e senha de arquivos eletrônicos etc.), além de procedimentos de outorga de guarda/transferência de bens, complementados por inventários periódicos e comparação com registros patrimoniais e de controle.

Atividades de controle específicas para Sistemas de Tecnologia da Informação

As organizações em todos os setores estão cada vez mais dependentes dos recursos de Tecnologia da Informação (TI) para conduzir os negócios, alcançar objetivos e cumprir suas missões. Um fator crítico dessa nova realidade é o uso eficiente e seguro desses recursos.

A informação e a tecnologia que lhe dá suporte é hoje, para a maioria das organizações, um ativo valioso. Em muitos casos, há uma dependência crítica dos processos organizacionais suportados por TI, exigindo-se uma adequada gestão de riscos e uma crescente necessidade de controle sobre as informações, fatores hoje considerados elementos-chave na governança corporativa.

Conforme já visto nesta aula, existem modelos específicos que se adéquam e dão suporte ao Coso no gerenciamento de riscos e na avaliação de controles na área de TI, sendo CobiT e ITIL as referências mais recomendadas, inclusive pela Intosai (2004, p.35). Não adentraremos em detalhes desses modelos, que requerem cursos específicos para sua abordagem, apenas destacaremos os dois grupos amplos de atividades de controle dos sistemas de informação, reconhecidos tanto pelo Coso, como pela Intosai e o GAO como "controles gerais de TI" e "controles de aplicativos de TI".

Os **controles gerais de TI** abrangem a estrutura, as políticas e os procedimentos aplicáveis a todos os sistemas de informação da organização, incluindo a totalidade dos componentes, desde a arquitetura de processamento – servidores, redes, estações etc. – até ambientes de usuários finais, com a finalidade de ajudar a assegurar uma operação adequada e contínua. Eles criam o ambiente no qual operam os sistemas aplicativos.

Os **controles de aplicativos de TI** abrangem a estrutura, as políticas e os procedimentos diretamente relacionados aos aplicativos corporativos individuais, incluindo procedimentos embutidos no código do programa, com a finalidade de ajudar a assegurar a integridade, precisão, autorização e validade de dados e transações neles processados.

Considerando que os controles específicos para sistemas de TI são objeto de cursos específicos, faremos a seguir apenas uma enumeração das principais categorias de atividades de controle contidas em cada um dos grupos de controle de TI, remetendo o leitor para um aprofundamento na bibliografia que é mencionada logo no início de cada um dos grupos de controle.

Controles gerais de TI

Segundo a Intosai (2004, p.33-34) e o GAO (p.56), há seis fatores ou categorias principais de atividades de controle que precisam ser consideradas ao se avaliar os controles gerais de TI:

1. Programa de planejamento e gestão da segurança de TI
2. Controles de acesso
3. Controles de desenvolvimento, manutenção e mudança em sistemas
4. Controles sobre aplicativos
5. Segregação de funções
6. Continuidade dos serviços

Controles de aplicativos de TI

Segundo a Intosai (2004, p.34) e o GAO (p.52), há quatro fatores ou categorias principais de atividades de controle que precisam ser consideradas ao se avaliar os controles de aplicativos de TI:

1. Controles de autorização
2. Controles de integralidade
3. Controles de precisão
4. Controles de integridade do processamento e dos arquivos de dados

Os controles gerais e os controles de aplicativos de TI, em conjunto com processos de controle manual, quando necessários (como políticas e procedimentos associados a atividades de usuários), devem se inter-relacionar. Todos são necessários para assegurar a integridade, a precisão e a validade das informações.

2.3.7. Informação e comunicação

A importância do controle interno para a gestão das organizações está no seu potencial informativo para dar suporte ao processo decisório em todos os níveis, de maneira que todos possam cumprir

suas responsabilidades, favorecendo o alcance dos objetivos. Todos na organização devem receber mensagens claras quanto ao seu papel e ao modo como suas atividades influenciam e se relacionam com o trabalho dos demais na consecução dos objetivos fixados.

A habilidade da administração para tomar decisões apropriadas é afetada pela **qualidade da informação**, que deve ser **apropriada**, **oportuna**, **atual**, **precisa** e **acessível**, fluindo do nível da administração para o nível de execução – transmitindo diretrizes e correções de rumo – e no sentido inverso – transmitindo dados e resultados relacionados aos objetivos perseguidos.

Para avaliar a qualidade da informação é necessário verificar se ela é:

Apropriada – o conteúdo está no nível de detalhes adequado?

Oportuna – está disponível quando necessária?

Atual – são as mais recentes ou a última versão disponível?

Precisa – os dados estão corretos?

Acessível – são de fácil obtenção por aqueles que as necessitam?

Os sistemas de informação registram, tratam e produzem relatórios contendo informações financeiras e não financeiras, nas formas quantitativas e qualitativas, que tornam possíveis a condução e o controle dos negócios. Informações relevantes devem ser identificadas, coletadas e comunicadas a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisões gerenciais.

A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam à informação fluir em todos os sentidos. A informação gerada no curso das operações é usualmente comunicada por meios de canais normais, para quem é o responsável e também para um nível superior ao desse. Contudo, canais alternativos de comunicação devem existir para transmitir informação delicada, como atos ilegais ou incorretos e comunicação de riscos.

Além das comunicações internas, a administração deve assegurar que existam meios adequados de se comunicar e de obter informações externas, uma vez que as comunicações externas podem fornecer insumos

de impacto significativo na extensão em que a organização alcança seus objetivos. Um plano de comunicação entre os níveis hierárquicos, bem como um plano de comunicação com outras partes interessadas (clientes, fornecedores, acionistas, sociedade etc.) é recomendável.

Meios de comunicação

A comunicação pode ser feita em diversos meios, como manuais de políticas e procedimentos, memorandos, mensagens de correio eletrônico, quadro de avisos, videoconferências, vídeos institucionais, páginas na internet/intranet, blogs, canais de redes sociais.

As políticas e procedimentos relacionados às atividades de controle e as regras internas necessárias ao funcionamento da entidade, tais como políticas corporativas, procedimentos e fluxos operacionais, funções e responsabilidades devem ser formalmente comunicadas por meio de instrumentos de normatização interna, com fácil acesso aos funcionários.

2.3.8. Monitoramento

Com o passar do tempo os objetivos e os riscos organizacionais podem mudar, respostas a riscos que se mostravam eficazes podem tornar-se inócuas e atividades de controle podem perder a eficácia ou deixar de ser executadas, colocando em risco objetivos da organização. Por isso, sistemas de controle interno devem ser monitorados para ver se permanecem eficazes.

O objetivo do monitoramento é avaliar a qualidade do controle interno ao longo do tempo, buscando assegurar que ele continue a funcionar efetivamente como previsto, que as respostas aos riscos e as atividades de controle sejam modificadas apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos da organização e das atividades por ela desenvolvidas.

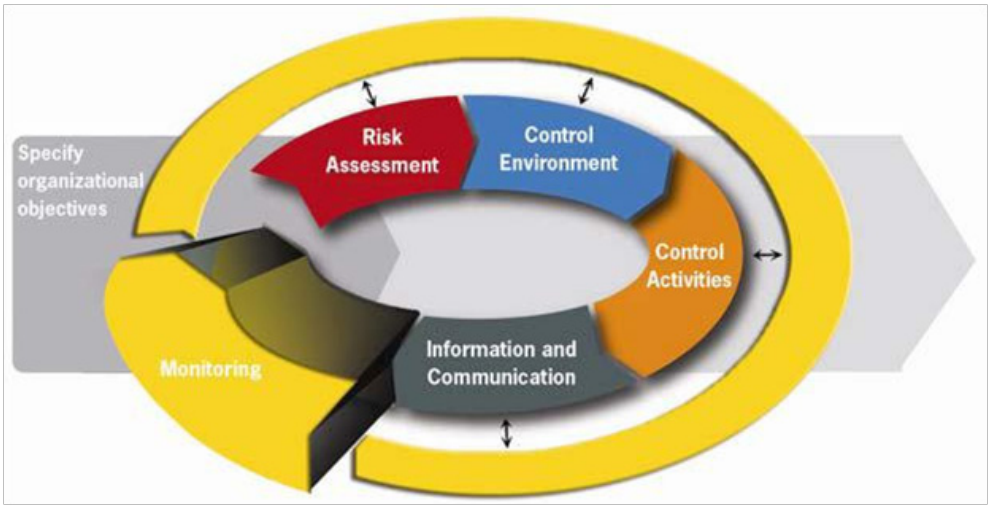
A avaliação de controles internos é o procedimento utilizado para realizar o monitoramento e consiste em verificar a eficácia do sistema de controle interno (em nível de entidade) e das atividades de controle inerentes aos processos (em nível de atividades).

A eficácia do controle interno é avaliada em relação aos cinco componentes do controle interno do Coso I ou, quando integrado ao gerencimento de riscos, aos oito componentes do Coso II. Determinar se um sistema de controlo interno é eficaz é um julgamento subjetivo resultante de uma avaliação sobre se cada um dos componentes está presente e se todos estão operando em conjunto.

A **adequação** diz respeito à concepção ou ao desenho do controle e o **funcionamento** diz respeito à sua aplicação eficaz, de maneira contínua e coerente.

Assim, o processo de monitoramento envolve a avaliação sobre a **adequação** e o **funcionamento** dos controles e considera a eficácia coletiva de todos os componentes do controle interno. Ou seja, se todos estão presentes e em funcionamento.

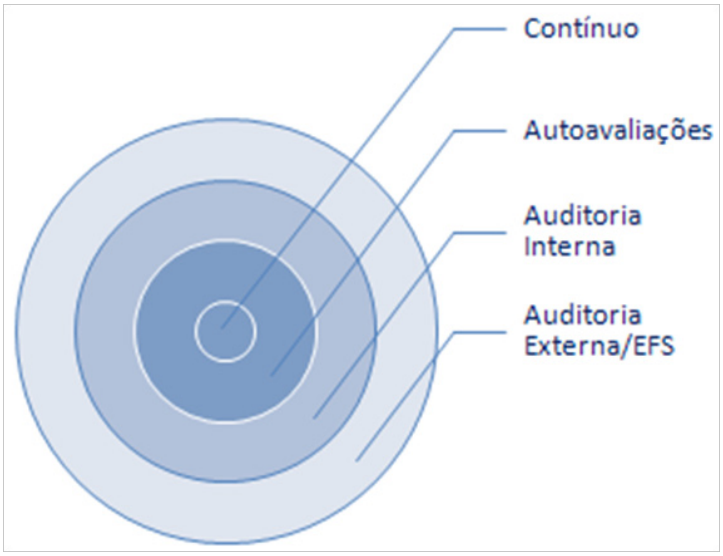
O monitoramento pode ser realizado de duas maneiras ou por uma combinação de ambas:



Monitoramento contínuo – por meio de atividades gerenciais contínuas, no curso das operações normais da organização.

Neste curso, a nossa ênfase são as **avaliações separadas**, mas não as autoavaliações.

Avaliações separadas – avaliações de controle interno, periódicas, por meio de autoavaliações e/ou de avaliações/revisões independentes executadas pela auditoria interna. Avaliações separadas podem também ser executadas pelas EFS e por auditores externos (INTOSAI, 2004, p. 41).



Note, portanto, que o objetivo do monitoramento é voltado para o funcionamento do sistema e das atividades de controle, enquanto o objetivo dessas últimas é minimizar riscos nos processos ou nas operações da organização, isto é, nas atividades de execução. Podemos entender, assim, que o **monitoramento consiste em controles que monitoram outros controles**, incluindo o monitoramento contínuo, realizado pela administração, no curso normal das atividades, programas de autoavaliação, e as atividades relacionadas a controles internos da função de auditoria interna, do comitê de auditoria, bem como das EFS e dos auditores externos, que constituem as avaliações separadas, tratadas a seguir.

Monitoramento contínuo

O monitoramento contínuo é realizado pelo próprio corpo gerencial da organização e consiste em fazer o acompanhamento de determinadas informações que indicarão se os controles internos estão ou não funcionando de maneira eficaz. Tal acompanhamento pode ser feito por meio de análises de variância, comparações de informações provindas de fontes diversas, correlação de indicadores financeiros e operacionais etc.

Um exemplo de monitoramento contínuo realizado por meio de correlação de indicadores financeiros e operacionais pode ser ilustrado com uma empresa de transportes, na qual os gastos com combustíveis (indicador financeiro) devem manter direta correlação com a quilometragem rodada pela frota de veículos (indicador operacional). Esse exemplo demonstra também que ter um sistema de custos e realizar análises de desempenho constituem poderosas ferramentas de monitoramento contínuo de uma organização.

O 'monitoramento' contínuo dos controles internos não deve ser confundido com o componente 'atividades de controle'. Enquanto estas incidem sobre atividades, processos e operações para assegurar o cumprimento de políticas, procedimentos e outros requisitos em vigor, aquele tem como foco o próprio funcionamento dos controles.

No exemplo apresentado, a organização possivelmente dispõe de controles para autorizar abastecimentos, controles de rotas e registros de quilometragem, mas o monitoramento do consumo desproporcional de combustível é que vai indicar se tais controles estão sendo eficazes ou se estão ocorrendo falhas e anomalias como, por exemplo, fraudes, desvios e conluios.

Avaliações separadas

Nas avaliações separadas, o monitoramento pode ser feito por meio de autoavaliações – realizadas pela própria equipe responsável por atividades, processos ou operações – ou por meio de avaliações e revisões independentes realizadas pela auditoria interna ou externa, incluindo as EFS.

A abordagem e a profundidade dos procedimentos adotados por cada uma dessas entidades avaliadoras pode variar significativamente, dependendo dos objetivos específicos dos trabalhos. Naturalmente, os de maior profundidade são os realizados pela auditoria interna. As avaliações conduzidas pela auditoria externa e pelas EFS podem ter menos profundidade se puderem utilizar a avaliação e os resultados dos trabalhos realizados pela auditoria interna. Para isso, os trabalhos dos auditores externos, inclusive das EFS, devem incluir uma análise da consistência e qualidade das avaliações feitas pela auditoria interna.

Autoavaliações

A autoavaliação de controles, (também conhecida como *control self-assessment* – CSA) foi desenvolvida inicialmente no Canadá. Trata-se de uma metodologia utilizada para avaliação e revisão dos principais objetivos de negócios da organização, dos riscos envolvidos na busca de atingir esses objetivos, bem como da eficácia dos controles internos adotados para administrar esses riscos.

O Instituto dos Auditores Internos (iiabrasil.org.br) tem uma certificação específica em CSA.

A metodologia é aplicada por meio de reuniões nas quais são utilizados questionários de autoanálise e outras ferramentas e técnicas para a condução e documentação do trabalho, com a facilitação de um auditor especialista em CSA. Cada área elege um avaliador e um responsável que a represente. O avaliador fica responsável por realizar a avaliação em seu setor e o gerente em aprovar o seu trabalho.

As reuniões ocorrem com a participação do gestor, de seus principais colaboradores e ainda dos clientes e fornecedores da área ou do processo organizacional objeto da autoavaliação, que discutem as questões propostas e respondem aos questionários de autoavaliação. No final, é elaborada a documentação de avaliação, na qual o gestor define se o risco é aceitável ou não, se os controles são suficientes ou se é necessário elaborar algum plano de ação para solucionar os problemas identificados.

Os questionários de autoanálise são elaborados objetivando levar os agentes envolvidos a uma reflexão e a formar um juízo sobre o cumprimento dos critérios avaliados, permitir identificar a existência de controles e a aderência deles às práticas adequadas, os principais pontos

fortes e fracos da área ou do processo organizacional e as causas das deficiências, tudo isso com o propósito de, ao final, estabelecer planos de ação para melhorias, de modo consensual, legitimados por todos.

Essa forma de monitoramento se propõe a interiorizar uma cultura de risco e controle nos servidores da organização, fazendo com que o próprio gestor e os seus colaboradores consigam avaliar se a sua área ou o seu processo de trabalho está ou não aderente às melhores práticas de controle interno, com os riscos adequadamente gerenciados.

O processo de CSA pode agilizar o trabalho de avaliação da auditoria interna, combinando-se os procedimentos de revisão da auditoria com os da autoavaliação. Para isso, o trabalho de CSA deve ser acompanhado pela auditoria, sendo recomendável a sua participação no desenvolvimento das ferramentas de autoavaliação e no acompanhamento da execução, como facilitadora, bem como na avaliação dos resultados. É recomendável, ainda, que implementação dos planos de ação decorrentes de autoavaliações sejam incorporados nos acompanhamentos (*follow-up*) da auditoria interna.

Avaliações separadas realizadas pela Auditoria Interna

Embora ainda pouco usual, os trabalhos de avaliação de controles internos realizados pelos órgãos de controle interno e de auditoria interna da administração pública federal tendem a aumentar substancialmente. Isto porque, como vimos na aula 1, a auditoria interna tem a atribuição precípua de auxiliar a monitorar a eficácia do controle interno mediante avaliações e recomendações endereçadas à administração, sendo este, inclusive, um dos objetivos fundamentais do Sistema de Controle Interno do Poder Executivo.

O TCU, como também vimos, está intensificando ações para promover a melhoria da gestão de riscos e controles internos na administração pública e, em função disso, passou a incluir, nas Decisões Normativas de prestação de contas, exigências de autoavaliações por parte dos gestores de órgãos e entidades públicos, bem como de avaliações separadas pelos órgãos de controle interno e pelas auditorias internas. Antes, o Acórdão TCU 1.074/2009 (BRASIL, 2009) já havia expedido recomendações a mais de 60 órgãos e entidades da administração pública para que normatizassem "a atividade de auditoria interna pelo menos quanto aos seguintes aspectos:" (grifamos).

Relatório, Voto e Acórdão 1.074/2009-Plenário, disponível na biblioteca do curso, pasta Material complementar.

> *9.1.2.3. âmbito de atuação das atividades de auditoria interna, inclusive quanto à* ***realização de trabalhos de avaliação de sistemas de controles internos****;*

9.1.3. ***realizem auditorias de avaliação de sistemas de controles internos.***

Dado o seu papel de auxiliar a organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança, conforme a própria definição da atividade de auditoria interna do IIA, a abordagem e profundidade dos procedimentos de avaliação da auditoria interna são maiores do que os de auditores externos, mesmo quando combinados com trabalhos de CSA.

A metodologia de avaliação apresentada nas aulas subsequentes deste curso, com abordagem aprofundada, é apropriada para avaliações da auditoria interna (ou das EFS, a depender dos objetivos e escopo do trabalho. Para estas, apresentamos o método baseado em QACI, que muitas vezes atende o alcance dos trabalhos mais comuns). Contudo, os auditores de controle externo precisam conhecê-la para poder avaliar a consistência e qualidade dos trabalhos realizados pela auditoria interna e decidir se podem neles se apoiar, bem como para, a partir dela, desenvolver procedimentos mais simplificados para seus próprios trabalhos de avaliação.

Avaliações separadas realizadas pela Auditoria Externa

Normalmente, os trabalhos da auditoria externa independente têm o objetivo de expressar uma opinião sobre as demonstrações contábeis e é no contexto desse objetivo que as avaliações de controle interno são realizadas pelos auditores externos.

No Brasil, as responsabilidades dos auditores independentes, no que diz respeito ao controle interno, foram estabelecidas nas normas de auditoria NBC PA 265, 315 e 330, do Conselho Federal de Contabilidade.

Segundo a NBC PA 315:

> O objetivo do auditor é identificar e avaliar os riscos de distorção relevante independentemente se causada por fraude ou erro, nos níveis de demonstração contábil e afirmações, por meio do **entendimento da entidade e do seu ambiente, inclusive do controle interno da entidade**, proporcionando assim uma base para o planejamento e a implementação das respostas aos riscos identificados de distorção relevante. (grifamos).

Observe que a avaliação dos auditores independentes é feita com base no "*entendimento da entidade e do seu ambiente, inclusive do controle interno*" e tem um objetivo muito específico de proporcionar "*uma base para o planejamento e a implementação das respostas aos riscos identificados de distorção relevante*", isto é, para subsidiar o planejamento do seu trabalho de auditoria das demonstrações contábeis. **O objetivo do seu trabalho é expressar uma opinião sobre as demonstrações contábeis e não sobre a eficácia do controle interno**. Portanto, a sua consideração sobre o controle interno é tão somente naquilo que for relevante para a elaboração das demonstrações contábeis, com a finalidade de planejar procedimentos de auditoria.

Não obstante, a NBC PA 265 estabelece que as deficiências encontradas, se consideradas significativas, devem ser comunicadas à administração e aos órgãos de governança da organização. É por meio dessa comunicação que os auditores externos dão a sua contribuição para melhorar a eficácia do controle interno das entidades. Veja o que diz a NBC PA 265 (grifos nossos):

> 6. **O auditor deve comunicar tempestivamente por escrito as deficiências significativas de controle interno** identificadas durante a auditoria aos responsáveis pela governança.
> 11. [...]:
> (b) [...] O auditor deve especificamente explicar que [...]:
> (i) **o objetivo da auditoria era o de expressar uma opinião sobre as demonstrações contábeis**;
> (ii) **a auditoria incluiu a consideração do controle interno relevante para a elaboração das demonstrações contábeis com a finalidade de planejar procedimentos de auditoria** que são apropriados nas circunstâncias, **mas não para fins de expressar uma opinião sobre a eficácia do controle interno**;

Vale ressaltar que as regras sobre a responsabilidade dos auditores independentes das empresas brasileiras que possuam ações (ADR) negociadas no mercado norte-americano (EUA) são mais abrangentes do que as estabelecidas pelo CFC. Naquele país, a lei Sarbanes-Oxley (SOX), de 2002, na Seção 404 - "*Management Assessment of Internal Controls*" (Avaliação dos Controles Internos pela Administração), determina que os diretores (presidente e financeiro) avaliem e certifiquem a eficácia dos controles internos sobre relatórios financeiros e que o auditor independente emita um relatório, em separado, atestando a participação da administração na avaliação e certificação da eficácia desses controles e dos procedimentos executados.

Além disso, a SOX criou o *Public Company Accounting Oversight Board* (PCAOB, algo como Conselho de Supervisão de Contabilidade das Companhias Abertas), organismo que exerce a supervisão externa dos auditores independentes. Esse organismo emitiu a norma AS -5 (*Auditing Standard*, Jul/2007, substituindo a inicial AS-2, de 2002), estabelecendo requisitos e fornecendo diretrizes para os auditores independentes realizarem auditorias sobre a avaliação que a administração faz da eficácia dos controles internos sobre relatórios financeiros ("*auditoria dos controles internos sobre relatórios financeiros*") integradas com auditoria de demonstrações financeiras. Nestas normas, o PCAOB deixa claro que o objetivo do auditor nas auditorias de controles internos sobre relatórios financeiros é expressar uma opinião sobre a eficácia desses controles e que, embora essas auditorias devam ser integradas com as auditorias de demonstrações financeiras, seus objetivos não são idênticos, o que implica trabalhos separados.

A norma AS-2 do PCAOB (posteriormente substituída pela AS-5) exemplifica o Coso como uma boa maneira para definir a estrutura de controles internos e avaliar a sua eficácia e estabelece que cabe à administração:

- definir a estrutura de controle interno anualmente;
- avaliar o controle interno em nível da entidade, em bases anuais;
- documentar, anualmente, os controles internos considerados vitais para cada processo, aplicação, bem como para as classes de transações que podem ter um impacto relevante sobre os relatórios financeiros, avaliando as ausências e/ou falhas, para implementar ou corrigir;
- testar, anualmente, cada processo, aplicação ou categorias de transações consideradas de fundamental importância para o conjunto dos controles internos que amparam a emissão de relatórios financeiros.

Cabe ainda, à administração publicar relatórios afirmando:

- a responsabilidade da administração no estabelecimento e manutenção dos controles e procedimentos internos para a emissão dos relatórios financeiros;
- a avaliação acerca da eficácia dos controles e procedimentos internos para a emissão dos relatórios financeiros;

- que o auditor independente da companhia atestou e reportou a avaliação feita pela administração sobre a eficácia dos controles internos e procedimentos para a emissão dos relatórios.

Observa-se certa semelhança entre as exigências das normas americanas e aquelas estabelecidas pelo TCU em relação às suas unidades jurisdicionadas, ao exigir que os gestores informem sobre o funcionamento do sistema de controle interno no Relatório de Gestão (DN-TCU 108/2010, Anexo II, Parte A, item 9; Portaria-TCU 123/2011, item 9.1) e a auditoria interna informe, no Relatório de Auditoria de Gestão, a sua avaliação sobre o funcionamento do sistema de controle interno (DN-TCU 110/2010, Anexo III, Parte A, item 3).

Avaliações separadas realizadas pelas EFS

As avaliações separadas executadas pelas EFS ou por outras entidades externas de auditoria e controle governamental podem contribuir para a eficácia do controle interno e, segundo a Intosai (2004, p. 46), as obrigações desses entes externos sobre o controle interno são estabelecidas em suas competências e incluem a avaliação do funcionamento do sistema de controle interno e a comunicação à administração sobre seus achados, envolvendo:

- determinar a importância e o grau de sensibilidade ao risco ao qual os controles estão sendo dirigidos;
- identificar e compreender os controles relevantes;
- determinar o que já se conhece sobre a eficácia do controle;
- avaliar a suscetibilidade do mal uso de recursos, as deficiências no alcance dos objetivos relacionados à ética, economia, eficiência e eficácia ou falhas na prestação de contas (accountability) e o descumprimento de leis e regulamentos;
- avaliar a adequação do desenho do controle;
- determinar, mediante testes, se os controles são eficazes;
- relatar sobre as avaliações do controle interno e discutir as ações corretivas necessárias.

Importante destacar que a avaliação de controles internos realizadas pelas EFS não se restringe à finalidade de planejar procedimentos de auditoria, como é o caso daquelas executadas pela

auditoria externa. No setor público, essas avaliações tanto servem a esse propósito, como também são realizadas com objetivos específicos de contribuir para a melhoria da governança, da gestão de riscos e dos sistemas de controle interno dos órgãos e das entidades que compõem a administração pública. Este curso foi desenvolvido precipuamente para dar suporte a essa última finalidade, sem prejuízo de que a sua metodologia também possa, com as adaptações e simplificações necessárias, atender a primeira.

As avaliações realizadas para determinar a extensão e o alcance de auditorias, ou seja, com a finalidade de planejar procedimentos de auditoria, são previstas na ISSAI 300, 3.1 a 3.4, segundo a qual a profundidade dos exames é determinada conforme o grau de confiabilidade que se pode atribuir aos controles internos do objeto que será auditado.

Ainda conforme essa norma, a profundidade dos procedimentos desse tipo de avaliação depende dos objetivos e do escopo da auditoria em questão, recaindo sobre controles diferentes de acordo com o tipo de auditoria:

Em **auditorias contábeis** recai sobre os controles destinados à salvaguarda de ativos e recursos e à garantia de exatidão e integridade dos registros contábeis. A avaliação focará os riscos e controles relacionados às contas contábeis e à preparação das demonstrações financeiras, incidindo, por exemplo, sobre os ciclos de receitas, compras, estocagem, patrimônio, tesouraria, folha de pagamento, gestão de informação.

Em **auditorias de conformidade** recai principalmente sobre os controles que auxiliam a administração no cumprimento de leis e regulamentos relacionados ao objeto da auditoria. A avaliação focará, por exemplo, os riscos e controles da área de licitações e contratos.

Em **auditorias operacionais** recai sobre os controles que ajudam a entidade ou o programa fiscalizado a desempenhar suas atividades de modo econômico, eficiente, eficaz e efetivo, garantido aderência à orientação política da administração e fornecendo informações financeiras e de gestão oportunas e confiáveis. A avaliação focará, por exemplo, os controles de riscos que possam afetar a eficácia e efetividade do programa governamental.

Para finalizar a abordagem da Intosai em relação às avaliações separadas, convém fixar que as normas dessa organização que tratam das avaliações destinadas a contribuir para a melhoria da governança, da gestão de riscos e dos sistemas de controle interno são a INTOSAI GOV 9100/2004, que é baseada no Coso I, e a INTOSAI GOV 9130/2007, que é baseada no Coso II. A ISSAI 300 trata do estudo e da avaliação do controle interno destinada a determinar a extensão e o escopo de auditorias.

Veremos, a seguir, como o assunto é tratado nas normas do TCU.

As NAT tratam as avaliações separadas levando em conta três situações:

- subsidiar a proposição de auditorias (NAT, 71);
- subsidiar o planejamento da auditoria (NAT, 71.1);
- contribuir para a melhoria da governança, da gestão de riscos e dos sistemas de controle interno (NAT, 72).

Em relação ao primeiro caso, acima mencionado, o conhecimento sobre os objetivos, riscos e controles relacionados ao objeto que possivelmente venha a ser auditado é obtido tipicamente por meio de levantamentos, que visam a conhecer a organização e o funcionamento de órgãos/entidades, sistemas, programas, projetos ou atividades governamentais, seguindo o documento Padrões de Levantamento.

No segundo caso, a avaliação é realizada dentro da fase de planejamento do próprio trabalho de auditoria que está sendo realizada, caso ela tenha sido proposta sem que as informações relativas aos objetivos, riscos e controles do objeto auditado estejam disponíveis, ou seja, não tenham sido obtidas pela forma anterior.

O terceiro caso refere-se às avaliações realizadas por meio de trabalhos específicos para contribuir com a melhoria da governança, da gestão de riscos e dos sistemas de controle interno. Essas avaliações, segundo das NAT, visam a avaliar o grau em que o controle interno de organizações, programas e atividades governamentais assegura, de forma razoável, que na consecução de suas missões, objetivos e metas, os princípios constitucionais da administração pública serão obedecidos e os seguintes objetivos de controle serão atendidos:

I. eficiência, eficácia e efetividade operacional, mediante execução ordenada, ética e econômica das operações;

II. integridade e confiabilidade da informação produzida e sua disponibilidade para a tomada de decisões e para o cumprimento de obrigações *accountability*;

III. conformidade com leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria instituição;

IV. adequada salvaguarda e proteção de bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.

Escopo e frequência das avaliações

As avaliações de controle interno variam em escopo e frequência, dependendo da relevância dos riscos e da importância dos controles na sua redução. Para certificar-se da eficácia do controle interno, as áreas de maior risco e as respostas a riscos de alta prioridade tendem a ser avaliadas com mais frequência, tanto em termos de desenho dos controles como de efetividade operacional, isto é, da concepção e regular aplicação e da capacidade de evitar a ocorrência de eventos, sendo estas avaliações realizadas por meio dos chamados testes de controle, que serão abordados nas aulas subsequentes.

A periodicidade das avaliações separadas depende também de regulamentações de órgãos de controle e supervisão ou de legislações específicas. O Banco Central do Brasil e a SOX, por exemplo, exigem certificações e avaliações anuais; no setor público, como vimos, o TCU incluiu exigências nas normas relativas à prestação de contas anuais, que na prática implicam a definição e revisão anual da estrutura de controle interno por parte da administração e a avaliação em nível da entidade.

O alcance da avaliação depende ainda das categorias de objetivos abordados – estratégicos, operacionais, comunicação e conformidade, pois os riscos e controles em relação a cada uma dessas categorias variam em quantidade e complexidade. Note, por exemplo, que a avaliação dos auditores independentes preocupa-se, sobretudo, com o objetivo 'comunicação', no aspecto relacionado às demonstrações contábeis ou relatórios financeiros.

No caso de autoavaliações, o principal gestor das unidades básicas organizacionais avalia pessoalmente os riscos e controles associados às

opções estratégicas e aos objetivos de alto nível, além do componente de ambiente interno; os gestores das várias atividades operacionais das unidades básicas avaliam a eficácia dos componentes em relação às suas esferas de responsabilidade; os auditores internos, normalmente, enfocam a estrutura global ou divisional, bem como as atividades-chave (processos e operações) priorizadas em função da relevância dos riscos para o alcance dos objetivos estabelecidos, em regime de ciclos de auditoria.

Por razões de custo e racionalização de esforços, é recomendável utilizar uma combinação de maneiras na realização de procedimentos de monitoramento que a administração julgue necessários e a auditoria julgue adequados para assegurar que o controle interno estabelecido forneça uma razoável segurança para o alcance dos objetivos pretendidos.

Comunicação de deficiências

As ausências ou deficiências do sistema de controle interno são detectadas por meio de procedimentos de monitoramento contínuo ou de avaliações separadas, e todas as deficiências (condição, real ou potencial, que possa afetar o alcance de objetivos) ou oportunidades para fortalecer o controle interno (aumentar as probabilidades de alcance dos objetivos) devem ser comunicadas às pessoas que possam adotar as ações necessárias.

As comunicações de deficiências variam de acordo com diversas circunstâncias. Internamente, a regra geral é que devem ser reportadas às pessoas com poder para determinar as ações corretivas. Vimos que os auditores externos devem comunicar por escrito aos responsáveis pela governança. No que tange a partes externas, a instituição deve observar as disposições contidas em regulamentações de órgãos de controle e supervisão ou de legislações específicas, como é o caso, por exemplo, das decisões normativas do TCU que tratam dos relatórios de gestão e dos relatórios de auditoria de gestão.

Para concluir esta aula, ressaltamos que a avaliação de controles internos, nos moldes concebidos pelo Coso e encampados por outras normas e regulamentações (SOX, PCAOB, Intosai, Basileia, ABNT ISO 31000/2009 etc.) ainda é relativamente nova e apresenta-se em desenvolvimento, por isso, as abordagens metodológicas adotadas pelas entidades que realizam avaliações ainda não apresentam um grau de padronização entre si.

Síntese

Nesta aula, estudamos os modelos de referência mais reconhecidos internacionalmente para a implementação e avaliação de controles internos. Percebemos que esses modelos são o ponto de partida para auxiliar na definição de estruturas customizadas para sistemas de controle interno de organizações diversas, evitando que se adote um conjunto descoordenado de controles, que não garantam efetivamente os benefícios desejáveis.

A implementação e manutenção de controles internos efetivos tornou-se uma preocupação crescente de governos, organismos profissionais e de instituições de controle, regulamentação e auditoria em todo o mundo, havendo exigências legais em relação às empresas que operam no mercado de capitais (SOX/PCAOB e CFC, por exemplo), às instituições financeiras (Basiléia, Banco Central do Brasil), bem como normas e diretrizes para entidades do setor público (Intosai, TCU, GAO).

Focamos o modelo Coso II para identificar os elementos de um controle interno eficaz, uma vez que a adoção desse modelo como padrão para controle interno, integrado ao gerenciamento de riscos, é uma tendência mundial. Vimos, ainda, que na área de TI, o modelo CobiT e a biblioteca de boas práticas Itil representam estruturas de controle especificas desenhadas para essa área, as quais complementam e dão suporte ao Coso, porém tais modelos não foram tratados em profundidade neste curso, por serem objeto de cursos específicos.

Estudamos detalhadamente os elementos que devem integrar um sistema de controle interno eficaz, tendo como referência o modelo Coso II, habilitando-nos a definir critérios para avaliação do controle interno em nível de entidade e fornecendo-nos importantes referenciais para avaliar controles internos em nível de atividades, operações e processos organizacionais específicos.

Por fim, ao estudarmos o último componente da estrutura Coso – o monitoramento – percebemos que a avaliação de controles internos é um procedimento que integra este componente da estrutura e, assim, integra o sistema de controle interno, como um instrumento para a sua eficácia.

Na próxima aula, estudaremos a avaliação do controle interno em nível da entidade.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR 31000 : 2009 : gestão de riscos: princípios e diretrizes. 1. ed. São Paulo, 2009.

_____. ABNT NBR ISO GUIA 73 : gestão de riscos : vocabulário. 1. ed. São Paulo, 2009.

AUSTRÁLIA; NOVA ZELÂNDIA. Standards. Committee OB-007. AS/NZS 4360:1999, Risk management. 2. ed. Sidney; Wellington, 1999.

BOYNTON, William; JOHNSON, Raymond; KELL, Walter. Auditoria. São Paulo: Atlas, 2002.

BRASIL. Ministério da Fazenda. Secretaria Federal de Controle Interno.

Manual do sistema de controle interno do poder executivo federal. Anexo à instrução normativa nº 01, de 6 de abril de 2001.Disponível em: <http://www.cgu.gov.br/Legislacao/Arquivos/InstrucoesNormativas/IN01_06abr2001.pdf>. Acesso em: 20 mar. 2010.

_____. Tribunal de Contas da União. Acórdão n.º 1074/2009, Plenário. Relator: Ministro Weder de Oliveira. Diário Oficial da União, Brasília, 22 maio 2009a. Disponível em: http://contas.tcu.gov.br/portaltextual/PesquisaFormulario?cmbTipoPesquisa=ACOR>. Acesso em: 03 nov. 2011.

_____. _____. Normas de Auditoria do Tribunal de Contas da União.

Revisão Junho 2011. Anexo à Portaria-TCU nº 280, de 8 de dezembro de 2010, alterada pela Portaria-TCU 168, de 30 de junho de 2011. Brasília, 2010a. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/PORTN/20110706/PRT2010-280.doc>. Acesso em: 1º ago. 2011.

_____._____. Instrução normativa – TCU nº 63, de 1º de setembro de 2010. Estabelece normas de organização e de apresentação dos relatórios de gestão e das peças complementares que constituirão os processos de contas da administração pública federal, para julgamento do Tribunal de Contas da União, nos termos do art. 7º da Lei nº 8.443, de 1992. Brasília, 2010b. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/IN/20100903/INT2010-063.rtf>. Acesso em: 1º ago. 2011.

_____._____. Decisão normativa – TCU nº 108, de 24 de novembro de 2010. Dispõe acerca das unidades jurisdicionadas cujos responsáveis

devem apresentar relatório de gestão referente ao exercício de 2011, especificando a organização, a forma, os conteúdos e os prazos de apresentação, nos termos do art. 3º da Instrução Normativa TCU nº 63, de 1º de setembro de 2010. Boletim do Tribunal de Contas da União Especial, Brasília, ano 43, n. 24, 2 dez. 2010d. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/DN/20101216/DNT2010-108.doc>. Acesso em: 1º ago. 2011.

_____._____. Decisão normativa – TCU nº 110, de 1º de dezembro de 2010. Dispõe acerca das unidades jurisdicionadas cujos responsáveis terão as contas de 2010 julgadas pelo Tribunal, especificando a forma, os prazos e os conteúdos das peças complementares que as comporão, nos termos dos arts. 4º, 5º, 9º e 13 da Instrução Normativa TCU nº 63, de 1º de setembro de 2010 . Boletim do Tribunal de Contas da União Especial, Brasília, ano 43, n. 27, 8 dez. 2010e. Disponível em: http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/DN/20101216/DNT2010-110.doc>. Acesso em: 1º ago. 2011.

_____._____. Portaria – TCU nº 123, de 12 de maio de 2011. Dispõe sobre orientações às unidades jurisdicionadas ao Tribunal quanto ao preenchimento dos conteúdos dos relatórios de gestão referentes ao exercício de 2011. Brasília, 2011a. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/PORTN/20110520/PRT2011-123.doc>. Acesso em 1º ago. 2011.

_____. Conselho Monetário Nacional. Resolução n.º 2.554 de 24 de setembro de 1998. Dispõe sobre a implantação e implementação de sistema de controles internos. Disponível em: <http://www.bcb.gov.br/ pre/normativos/res/1998/pdf/res_2554_v1_P.pdf>. Acesso em: 21 abr. 2009.

_____. _____. Resolução n.º 3.380 de 29 de junho de 2006. Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional. Disponível em: <http://www.bcb.gov.br/pre/normativos/res/2006/pdf/ res_3380_v1_P.pdf>. Acesso em: 21 abr. 2009.

_____. _____. Resolução n.º 3.721 de 30 de abril de 2009. Dispõe sobre a implementação de estrutura de gerenciamento do risco de crédito. Disponível em: <http://www.bcb.gov.br/pre/normativos/res/2009/pdf/res_3721.pdf>. Acesso em: 21 abr. 2009.

COMMITTE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), (Org.). Internal Control: integrated framework. United States of America: COSO, 1992. (Executive Summary). Disponível em <www.coso.org/IC-IntegratedFramework-summary.htm>. Acesso em: 21 abr. 2009.

_____. Gerenciamento de riscos corporativos: estrutura integrada. PriceWatherhouseCoopers, COSO, Audibra, Nov. 2006. (Sumário Executivo. Estrutura) Disponível em: <http://www.coso.org/documents/ COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em: 20 mar. 2010.

_____. Gerenciamento de riscos corporativos : estrutura integrada: técnicas de aplicação. PriceWatherhouseCoopers. COSO: Audibra, nov. 2006.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). Resolução CFC Nº. 1.135/2008. Aprova a NBC T 16.8 – Controle Interno. Disponível em: <http://www.cfc.org.br/sisweb/sre/docs/RES_1135.doc>. Acesso em: 20 mar. 2010.

_____. Resolução CFC Nº. 1.210/2009. Aprova a NBC PA 265 – Comunicação de deficiências de Controle Interno. Disponível em: < http://www.cfc.org.br/sisweb/sre/docs/RES_1210.doc>. Acesso em: 5 out. 2011.

_____. Resolução CFC Nº. 1.212/2009. Aprova a NBC PA 315 – Identificação e avaliação dos riscos de distorção relevante por meio do entendimento da entidade e do seu ambiente. Disponível em: < http://www.cfc.org.br/sisweb/sre/docs/RES_1212.doc>. Acesso em: 5 out. 2011.

_____. Resolução CFC Nº. 1.214/2009. Aprova a NBC PA 330 – Resposta do auditor aos riscos avaliados. Disponível em: < http://www.cfc.org.br/ sisweb/sre/docs/RES_1214.doc>. Acesso em: 5 out. 2011.

DAVIS, Marcelo David; BLASCHEK, José Roberto de Souza. Deficiências dos sistemas decontrole interno governamentais atuais em função da evolução da economia. In: CONGRESSO USP DE CONTROLADORIA E CONTABILIDADE, 6., 2006. Anais… São Paulo: Universidade de São Paulo, 2006.

ESTADOS UNIDOS. Government Accountability Office (GAO). GAO-01-1008G: ferramenta de gestão e avaliação de controle interno. Washington, D.C: Government Accountability Office, 2001.

_____. GAO-01-1008G: internal control management and evaluation tool. Aug. 2001. Disponível em: <http://www.gao.gov/new.items/d011008g.pdf>. Acesso em: 19 de abr. 2009.

FEDERAÇÃO BRASILEIRA DOS BANCOS (FEBRABAN). Análise das ferramentas de autoavaliação na gestão do risco operacional. Dez.

2004. Disponível em: <http://www.febraban.org.br/Arquivo/Destaques/CSA-%20041223.pdf>. Acesso em: 29 set. 2011

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. Implantando a governança de TI: da estratégia à gestão dos processos e serviços. 2. ed. - Rio de Janeiro: Brasport, 2008.

INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). Normas internacionais de auditoria das Entidades de Fiscalização Superior (ISSAI). Disponível em: <http://www. issai.org/composite-347.htm>. Acesso em 20 mar. 2010.

_____. GOV 9100 Guidelines for Internal Controls Standards for the Public Sector. 2004. Disponível em: <http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsece.pdf>. Acesso em 21 abr. 2009.

_____. GOV 9130 Guidelines for Internal Controls Standards for the Public Sector: further information on entity risk management. PSC Subcommittee on Internal Control Standards. 2007. Disponível em: < http://psc.rigsrevisionen.dk/composite-218.htm>. Acesso em: 21 abr. 2009.

IT GOVERNANCE INSTITUTE. CobiT® 4.1. ITGI: 2007, tradução e revisão do Projeto CobiT-BR Disponível em < http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf>. Acesso em: 1 ago. 2011.

KRIECK, Charles; COSTA, Flora Steuer. Auditoria em ambiente de ERP (Sistemas de gestão integrados). Elaboração: KPMG Auditores Independentes. In: SILVA, José Barbosa da (coord.). Auditoria em ambiente de internet. São Paulo : Atlas, 2001 (Coleção Seminários CRC-SP/Ibracon).

MARTINS, N. C.; SANTOS, L. R.; DIAS FILHO, J. M. Governança empresarial, riscos e controles internos: a emergência de um novo modelo de controladoria. Revista Contabilidade & Finanças, São Paulo, n. 34, p. 7-22, jan./abr. 2004.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). An audit of internal control over financial reporting that is integrated with an audit of financial statements. New York: PCAOB, 2007. (Auditing Standard, no. 5) Disponível em: <http://pcaobus.org/Standards/ Auditing/Pages/Auditing_Standard_5.aspx>. Acesso em 06 out. 2011.