KPMG
cutting through complexity

Mesa de Debates das Mudanças Promovidas pelo COSO 2013

Desafios para Adotarmos os Princípios*

* Resultado da pesquisa interativa efetuada em 12 de março de 2015, durante o evento "Praticando o COSO 2013 - Estrutura Integrada"

kpmg.com/BR

Desde a sua criação, em 1992, o *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*- Estrutura Integrada teve uma ampla aceitação por parte dos responsáveis pela elaboração e pela avaliação dos controles internos corporativos. Empresas de capital aberto e outras entidades no mundo inteiro utilizam-na para avaliar e documentar a eficácia de seus sistemas de controle interno, especialmente aqueles relacionados à elaboração de relatórios financeiros — *Internal Control Over Financial Reporting (ICOFR)*.

A partir de 15 de dezembro de 2014, o COSO 1992 foi substituído pelo COSO 2013, atualizado pelo Conselho Diretor do COSO para torná-lo cada vez mais relevante para investidores e acionistas em um ambiente de negócios dinâmico e em rápida evolução. A Estrutura Integrada COSO 2013 é, portanto, voltada para melhorias nas estruturas de controles das organizações no contexto de um ambiente de negócios em rápida evolução.

Em 12 de março de 2015, a KPMG no Brasil promoveu o evento "Praticando o COSO 2013 - Estrutura Integrada", no qual apresentamos as mudanças-chave da estrutura de 1992 para a estrutura de 2013 (enfoque no atendimento do *ICOFR*), incluindo as razões das mudanças, bem como as considerações sobre sua execução: (i) os 17 princípios que respaldam cada um dos cinco componentes do COSO e (ii) as implicações da

transição de uma organização para a estrutura de 2013, relativamente à avaliação da Administração sobre a eficácia dos controles internos na preparação e na divulgação de informações financeiras para fins regulatórios, incluindo *PCAOB Attentions* e *US Companies Adopted*.

Ademais, neste mesmo evento, aproveitamos para aplicar uma pesquisa interativa, questionando os participantes sobre "Qual seria o desafio para adotarmos/implementarmos os princípios em nossas Empresas" e, com satisfação, compartilhamos os resultados nesta lâmina.

Boa Leitura!

Diogo Dias
Sócio
Tel.: (11) 3940-4038
dsdias@kpmg.com.br

Leandro Augusto M. Antonio
Sócio
Tel.: (11) 3940-3740
lantonio@kpmg.com.br

Eduardo Ferreira
Sócio-diretor
Tel.: (11) 3940-4038
elouzada@kpmg.com.br


8942.08
8525.08
7691.08
7274.08
6857.08
6440.08
6023.08
5606.08
4772.08
4355.08
13.12
14.37

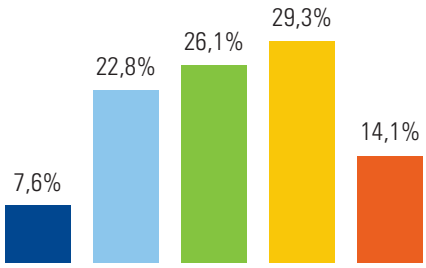
Resultado da Votação Interativa

A seguir apresentamos o resultado da pesquisa interativa, princípio a princípio:

1 A organização demonstra comprometimento com a integridade e a ética.

Qual seria o desafio para adotarmos/implementarmos o princípio 1 em nossas Empresas?

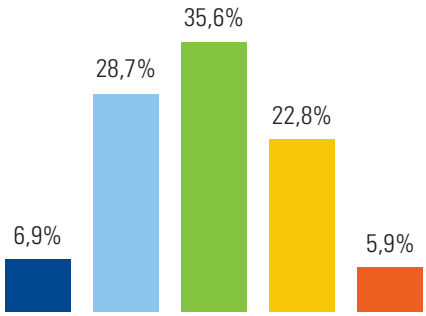
1. Evidenciar a publicação das normas ou dos códigos de conduta, incluindo políticas e procedimentos escritos, para todos os níveis da Empresa
2. Evidenciar a disseminação da filosofia e dos valores, estipulados pela Administração e pelo Conselho de Administração, para todos os níveis da Empresa
3. Evidenciar a comunicação, incluindo a rotineira e a informal, realizada por líderes em todos os níveis da Entidade
4. Evidenciar a resposta às violações às normas de conduta conforme estipulado pela Administração e pelo Conselho de Administração
5. NDA



2 O Conselho de Administração demonstra independência em relação à Administração, realizando uma supervisão da elaboração e da execução dos controles internos.

Qual seria o desafio para adotarmos/implementarmos o princípio 2 em nossas Empresas?

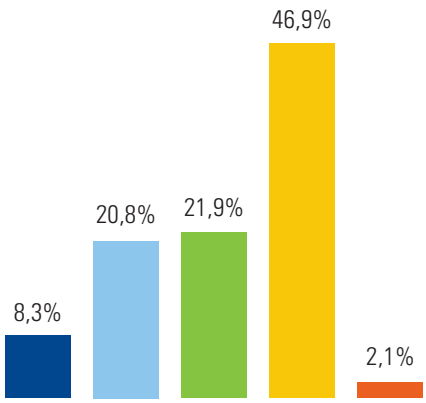
1. Documentar/evidenciar as atividades de monitoramento relacionadas aos controles internos sobre a preparação e a divulgação de informações financeiras
2. Documentar/evidenciar com profundidade as discussões sobre riscos futuros que possam impactar a preparação e a divulgação de informações financeiras
3. Documentar/evidenciar com detalhamento as análises realizadas sobre as informações recebidas (bases confiáveis, revisadas e corroboradas) que suportam a preparação
4. Documentar/evidenciar com efetividade a correção de deficiências identificadas nos controles internos sobre a preparação e a divulgação de informações financeiras
5. NDA



3 A Administração estabelece, com supervisão do Conselho de Administração, estruturas, quem responde para quem e os poderes e as responsabilidades adequados para a busca dos objetivos

Qual seria o desafio para adotarmos/implementarmos o princípio 3 em nossas Empresas?

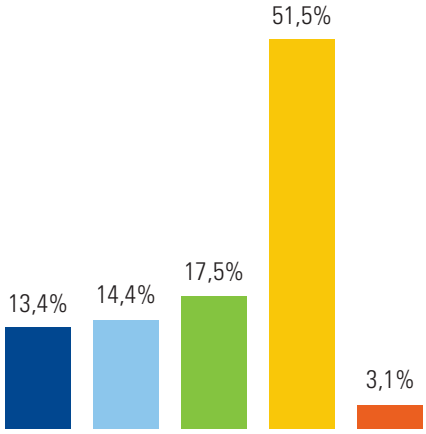
1. Estruturar canais de comunicação, formais e independentes, que realmente possibilitem a prestação de contas, tempestiva, das unidades de negócio e dos departamentos da Empresa
2. Estruturar canais de comunicação, formais e independentes, que realmente possibilitem a prestação de contas, tempestiva, dos subcontratados/terceirizados
3. Evidenciar a supervisão efetiva da Administração sobre as obrigações e os trabalhos (*assignments*) realizados pelas unidades de negócio e pelos departamentos da Empresa
4. Evidenciar a supervisão efetiva da Administração sobre as obrigações e os trabalhos (*assignments*) realizados pelos subcontratados/terceirizados
5. NDA



4 A organização demonstra comprometimento com a atração, o desenvolvimento e a retenção de indivíduos competentes em harmonia com os objetivos.

Qual seria o desafio para adotarmos/implementarmos o princípio 4 em nossas Empresas?

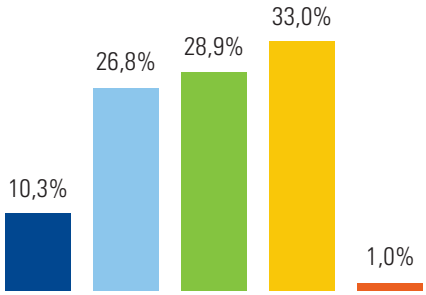
1. Documentar a avaliação da competência (habilidades e conhecimentos) da Alta Administração
2. Documentar o plano de sucessão da Alta Administração
3. Documentar a existência de especialistas nas "camadas" gerenciais da Empresa
4. Documentar a avaliação da competência (habilidades e conhecimentos) dos subcontratados/terceiros da Empresa
5. NDA



5 A organização responsabiliza os indivíduos pelos controles internos a eles atribuídos para a busca dos objetivos.

Qual seria o desafio para adotarmos/implementarmos o princípio 5 em nossas Empresas?

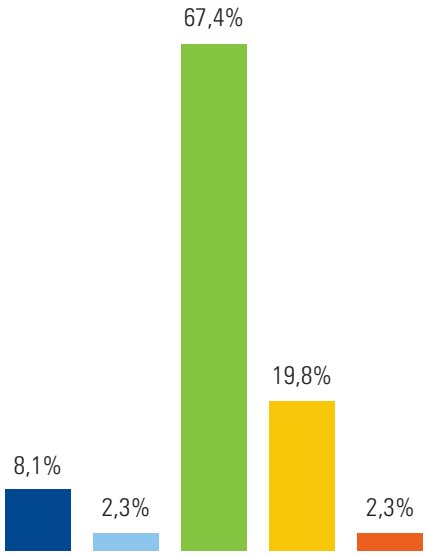
1. Incluir no programa de incentivo aos funcionários (PLR) a responsabilidade sobre os controles internos
2. Definição, pela Empresa, de regras do programa de incentivo aos funcionários (PLR) "balanceadas" entre medições financeiras (ex.: vendas) e não financeiras (ex: conduta ética)
3. Definição, pela Empresa, de regras do programa de incentivo aos funcionários (PLR) "balanceadas" entre objetivos/metas de curto e longo prazos — none excessive pressure
4. Definição, pela Empresa, de "mecanismos" (processos formais) para acompanhar seus empregados na execução efetiva de suas responsabilidades advindas do *ICOFR*
5. NDA



6 A organização especifica objetivos com suficiente clareza a fim de possibilitar a identificação e a avaliação dos riscos relacionados aos seus objetivos.

Qual seria o desafio para adotarmos/implementarmos o princípio 6 em nossas Empresas?

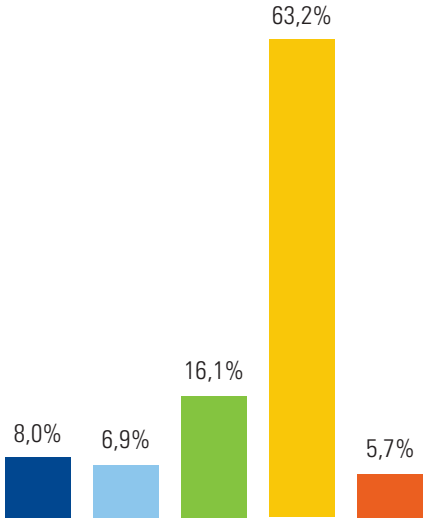
1. Identificar os objetivos que afetam as demonstrações financeiras
2. Definir a materialidade das demonstrações financeiras
3. Definir o risco de tolerância (precisão) dos controles internos
4. Documentar o processo de avaliação de riscos para o *ICOFR*
5. NDA



7 A organização identifica riscos para a realização de seus objetivos e analisa riscos como uma base para determinar como os riscos deveriam ser gerenciados.

Qual seria o desafio para adotarmos/implementarmos o princípio 7 em nossas Empresas?

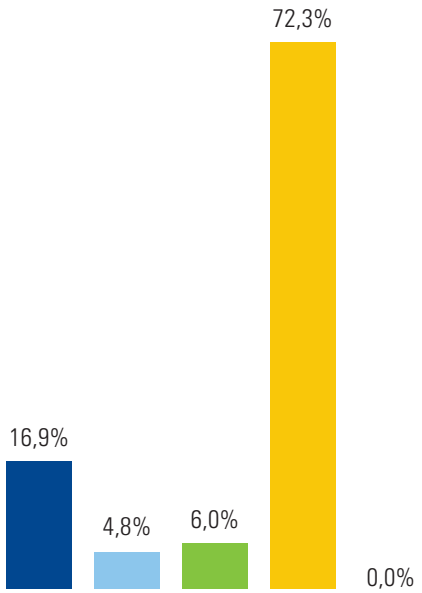
1. Identificar os riscos que afetam os objetivos de *ICOFR* da Empresa
2. Documentar a análise efetuada sobre os riscos que afetam os objetivos de *ICOFR* da Empresa
3. Documentar a resposta praticada sobre os riscos que afetam os objetivos de *ICOFR* da Empresa
4. Documentar o processo de identificação, avaliação e resposta aos riscos que afetam os objetivos de *ICOFR* da Empresa
5. ND



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

Qual seria o desafio para adotarmos/implementarmos o princípio 8 em nossas Empresas?

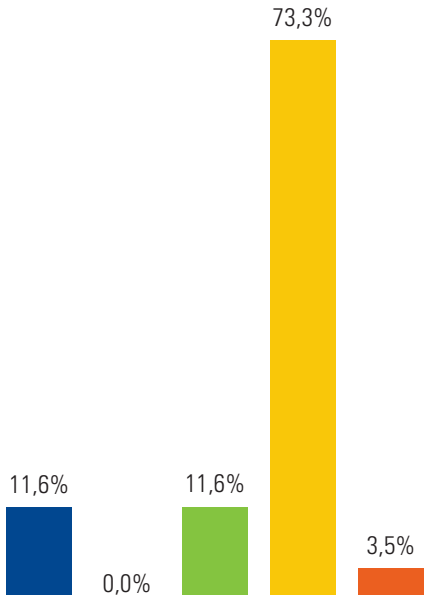
1. Identificar os riscos potenciais de fraude que possam afetar os objetivos de *ICOFR* da Empresa
2. Documentar a análise efetuada sobre os riscos potenciais de fraude que possam afetar os objetivos de *ICOFR* da Empresa
3. Documentar a resposta praticada sobre os riscos potenciais de fraude que possam afetar os objetivos de *ICOFR* da Empresa
4. Documentar o processo de identificação, avaliação e resposta aos riscos potenciais de fraude que possam afetar os objetivos de *ICOFR* da Empresa
5. NDA



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

Qual seria o desafio para adotarmos/implementarmos o princípio 9 em nossas Empresas?

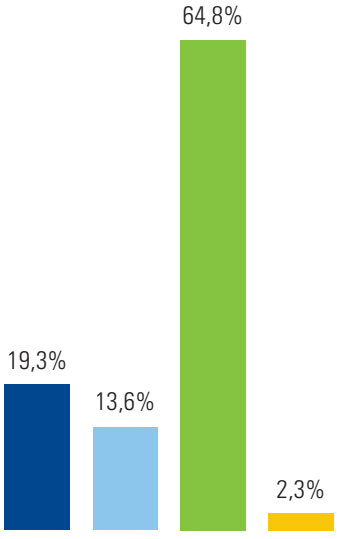
1. Identificar mudanças no ambiente de controles que possam afetar os objetivos de *ICOFR* da Empresa
2. Documentar a análise efetuada sobre as possíveis mudanças no ambiente de controles que possam afetar os objetivos de *ICOFR* da Empresa
3. Documentar a resposta praticada sobre as possíveis mudanças no ambiente de controles que possam afetar os objetivos de *ICOFR* da Empresa
4. Documentar o processo de identificação, avaliação e resposta às possíveis mudanças no ambiente de controles que possam afetar objetivos de *ICOFR* da Empresa
5. NDA



10 A organização seleciona e desenvolve atividades de controle que contribuem para a mitigação de riscos em níveis aceitáveis para a realização dos objetivos.

Qual seria o desafio para adotarmos/implementarmos o princípio 10 em nossas Empresas?

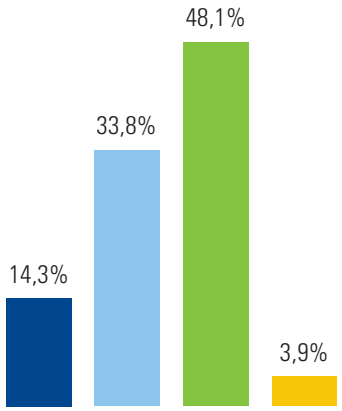
1. Identificar os Controles em Nível de Entidade (Entity-Level Controls) que mitigam os riscos a níveis aceitáveis para a realização dos objetivos do *ICOFR*
2. Identificar os Controles-chave em Nível de Transação (Transactional-Level Controls) que mitigam os riscos a níveis aceitáveis para a realização dos objetivos do *ICOFR*
3. Categorizar os Controles-chave em Nível de Transação (Transactional-Level Controls) em alto, médio ou baixo, considerando sua dependência de informações advindas de relatórios gerados via query ou planilhas eletrônicas
4. NDA



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

Qual seria o desafio para adotarmos/implementarmos o princípio 11 em nossas Empresas?

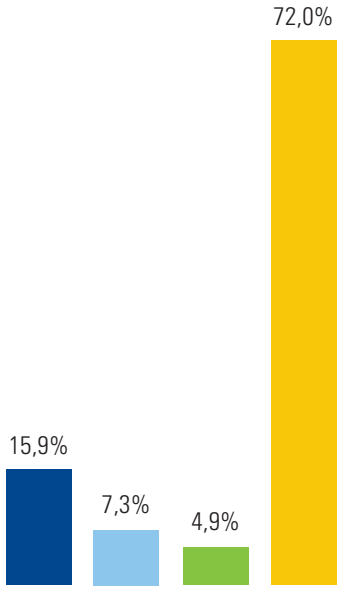
1. Identificar os sistemas e os Controles Gerais de Tecnologia relevantes para o atendimento dos objetivos do *ICOFR*
2. Vincular os Controles Automatizados, no Nível dos Processos, com os Controles Gerais de Tecnologia da Informação que respaldam as operações
3. Documentar a efetividade dos Controles Automatizados e dos Controles Gerais de Tecnologia da Informação que respaldam as operações
4. NDA



Quais são os passos para desenhar os controles gerenciais?

I. **Entender o processo em torno da revisão gerencial efetuada e os riscos relacionados**
II. **Identificar os controles que contribuam com a integridade e a exatidão da informação usada na revisão gerencial**
III. **Avaliar a habilidade e o conhecimento do profissional que executa a revisão gerencial**
IV. **Definir o nível de precisão na execução da revisão gerencial**

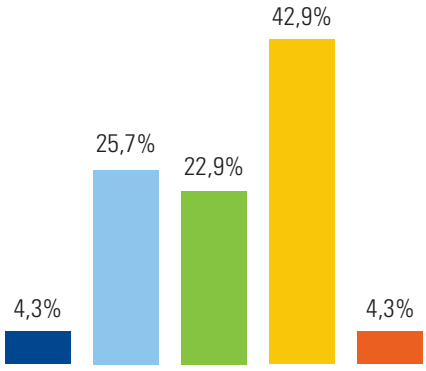
1. I, II e III somente
2. I, II e IV somente
3. I, III e IV somente
4. Todos



12 A organização realiza atividades de controle por meio de políticas que estabelecem o que é esperado em procedimentos que executam as políticas.

Qual seria o desafio para adotarmos/implementarmos o princípio 12 em nossas Empresas?

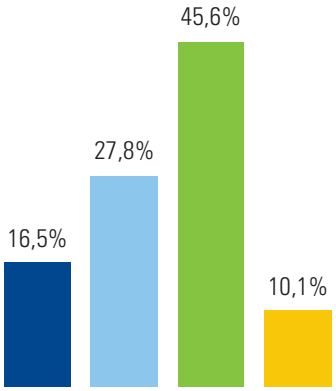
1. Entender o processo em torno da revisão gerencial efetuada e os riscos relacionados
2. Identificar os controles que contribuam com a integridade e a exatidão da informação usada na revisão gerencial
3. Avaliar a habilidade e o conhecimento do profissional que executa a revisão gerencial
4. Definir o nível de precisão na execução da revisão gerencial
5. NDA



13 A organização obtém/gera e usa informação relevante e de qualidade para suportar os outros componentes de controle interno.

Qual seria o desafio para adotarmos/implementarmos o princípio 13 em nossas Empresas?

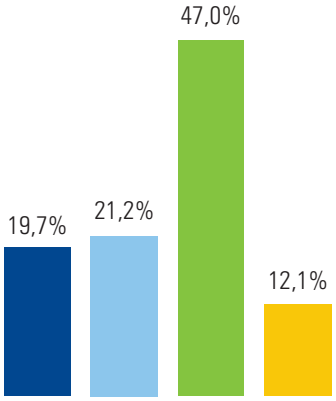
1. Inventariar as informações relevantes e de qualidade para suportar os componentes dos controles internos *(ICOFR)*
2. Suportar documentalmente as informações relevantes e de qualidade que contribuam com os componentes dos controles internos *(ICOFR)*
3. Formalizar a "corroboração" das informações relevantes e de qualidade por meio de reuniões e entrevistas
4. NDA



14 A organização comunica informações internamente, incluindo objetivos e responsabilidades para controle interno, necessários para suportar o funcionamento de outros componentes de controle interno.

Qual seria o desafio para adotarmos/implementarmos o princípio 14 em nossas Empresas?

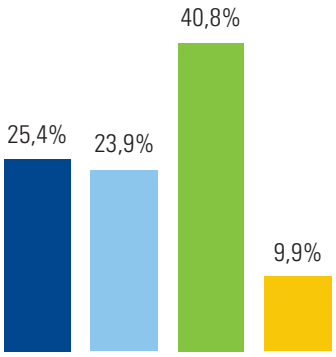
1. Definir a tempestividade que a Empresa deve efetuar a comunicação interna das informações relevantes e de qualidade para suportar os componentes dos controles internos *(ICOFR)*
2. Definir o tipo de comunicação (ex.: *e-mail*, Internet etc.) que a Empresa deve aplicar para que a comunicação seja objetiva e suporte os componentes dos controles internos *(ICOFR)*
3. Definir o público-alvo interno da Empresa que deve receber as comunicações para suportar os componentes dos controles internos *(ICOFR)*
4. NDA



15 A organização comunica-se com partes externas com relação a problemas que afetam o funcionamento de outros componentes de controle interno.

Qual seria o desafio para adotarmos/implementarmos o princípio 15 em nossas Empresas?

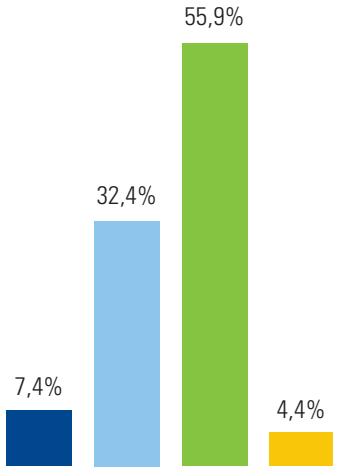
1. Definir a tempestividade que a Empresa deve efetuar a comunicação externa das informações relevantes e de qualidade para suportar os componentes dos controles internos *(ICOFR)*
2. Definir o tipo de comunicação (ex.: formulários, publicações, *press release*) que a Empresa deve aplicar para que a comunicação às partes externas seja "clara" sobre o funcionamento dos seus componentes dos controles internos *(ICOFR)*
3. Definir o público-alvo externo da Empresa que deve receber as comunicações sobre o funcionamento dos seus componentes dos controles internos *(ICOFR)*
4. NDA



16 A organização seleciona, desenvolve e efetua avaliações contínuas e/ou específicas para determinar se os componentes de controle interno estão presentes e em funcionamento.

Qual seria o desafio para adotarmos/implementarmos o princípio 16 em nossas Empresas?

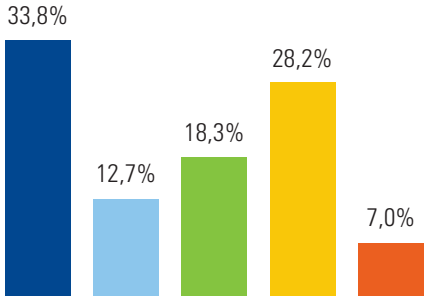
1. Definir a periodicidade da geração dos relatórios de monitoramento (avaliações contínuas e específicas) para que os riscos relacionados ao *ICOFR* sejam identificados, avaliados e respondidos rapidamente
2. Desenhar os relatórios de avaliações contínuas que podem antecipar possíveis mudanças nos negócios (ex.: aumento da inadimplência), auxiliando na detecção e/ou na correção de erros nas demonstrações financeiras
3. Desenhar os relatórios de avaliações específicas que podem antecipar mudanças nos processos (ex.: elevação na quantidade de produtos em estoque próximo da data de expiração), auxiliando na detecção e/ou na correção de erros nas demonstrações financeiras
4. NDA



17 A organização avalia e comunica deficiências de controle interno de maneira tempestiva para as partes responsáveis pela tomada de medidas corretivas, incluindo Alta Administração, quando apropriado.

Qual seria o desafio para adotarmos/implementarmos o princípio 17 em nossas Empresas?

1. Dificuldade em determinar a root cause da deficiência
2. Dificuldade em determinar a severidade (probabilidade) da deficiência
3. Dificuldade em determinar a severidade (impacto) da deficiência
4. Dificuldade em identificar controles compensatórios
5. NDA



Questões comentadas

Para melhor entendimento, apresentamos o resultado comentado da pesquisa interativa princípio a princípio, exceto para os seguintes, a seguir relacionados, que optamos por "responder agrupadamente" para auxiliar na compreensão de seu impacto como um todo no Ambiente de Controles Internos das Empresas.

- Princípios 2 e 13
- Princípios 3 e 4
- Princípios 6 e 12
- Princípios 7, 8 e 9
- Princípios 14 e 15

Questão 1

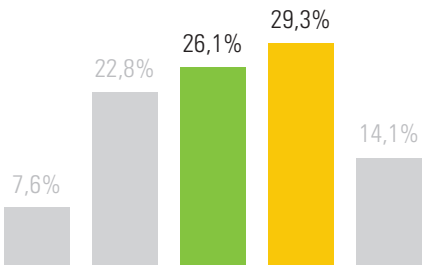
Qual seria o desafio para adotarmos/implementarmos o princípio 1 em nossas Empresas?

Evidenciar a resposta às violações às normas de conduta conforme estipulado pela Administração e pelo Conselho de Administração.

29,3%

Evidenciar a comunicação, incluindo a rotineira e a informal, realizada por líderes em todos os níveis da entidade.

26,1%



Princípio 1: A organização demonstra comprometimento com a integridade e a ética.

Para atendimento ao princípio 1, um dos aspectos que acreditamos que requer maior atenção para a transição das Empresas para a Estrutura Integrada COSO 2013 é que "todo o sistema de controle interno deve estar presente e funcionando em todos os níveis da Empresa". Logo, a Alta Administração deve avaliar e documentar o escopo apropriado para atendimento do *Internal Control Over Financial Reporting (ICOFR)*, que consiste em: (i) acessar os riscos de *material misstatement* nas suas demonstrações financeiras, associando-os a cada nível da Empresa; e (ii) desenhar e implementar adequados controles para os níveis da Empresa que endereçam esses riscos.

Deste modo, levando em consideração o resultado da pesquisa interativa efetuada, os dois maiores desafios encontrados para o atendimento deste princípio foram:

(a) "Evidenciar a resposta às violações às normas de conduta conforme estipulado pela Administração e pelo Conselho de Administração": para evidenciar a resposta a violações, a Alta Administração da Empresa deve estabelecer regras objetivas de conduta, bem como respostas diretas ao não atendimento dessas regras. Isto significa dizer que a Empresa não somente deve disponibilizar, por exemplo, seu Código de Conduta, mas também um guia de "penalidades" a serem aplicadas pelo não atendimento e "intervenções" tempestivas feitas , indicando quem auxilia a Alta Administração na "intervenção" e aplica o guia de "penalidades". A evidenciação deste processo dar-se-á por meio da documentação e da explicação do desvio diante da política pelo "interventor" e alinhado a "penalidade" aplicada de acordo com o estipulado no guia.

(b) "Evidenciar a comunicação, incluindo a rotineira e a informal, realizada por líderes em todos os níveis da entidade": para evidenciar a realização da comunicação, a Alta Administração da Empresa deve não somente evidenciar suas reuniões periódicas, como também usar seus meus de comunicação (ex.: *e-mails*, intranet etc.) para "comunicar-se direta e objetivamente com seus colaboradores", sempre que necessário — vide comentários adicionais na resposta aos princípios 2 e 13 (primeiro tópico).

Questão 2

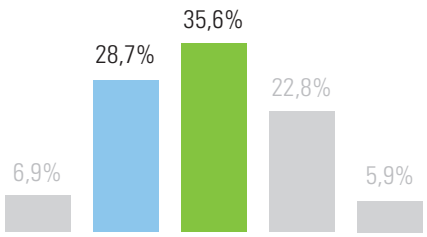
Qual seria o desafio para adotarmos/implementarmos o princípio 2 em nossas Empresas?

Documentar/evidenciar com detalhamento as análises realizadas sobre as informações recebidas (bases confiáveis, revisadas e corroboradas) que suportam a preparação e a divulgação de informações financeiras.

35,6%

Documentar/evidenciar com profundidade as discussões sobre riscos futuros que possam impactar a preparação e a divulgação de informações financeiras.

28,7%



Questão 13

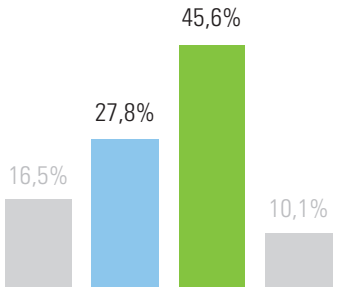
Qual seria o desafio para adotarmos/implementarmos o princípio 13 em nossas Empresas?

Formalizar a "corroboração" das informações relevantes e de qualidade por meio de reuniões e entrevistas.

45,6%

Suportar documentalmente as informações relevantes e de qualidade que contribuam com os componentes dos controles internos *(ICOFR)*.

27,8%



Princípio 2: O Conselho de Administração demonstra independência em relação à Administração, realizando uma supervisão da elaboração e da execução dos controles internos.

Princípio 13: A organização obtém/gera e usa informação relevante e de qualidade para suportar os outros componentes de controle interno.

Em relação ao princípio 2, a ênfase na Estrutura Integrada COSO 2013 é introduzir quatro pontos de atenção focados na necessidade de transparência de como as Empresas operam e "governam" elas mesmas, tendo como "meta" o atingimento do *Internal Control Over Financial Reporting (ICOFR)*.

Já o princípio 13 foca na "Empresa obtém/gera e usa informação relevante e de qualidade para suportar os outros componentes de controle interno".

No resultado da pesquisa interativa efetuada, os quatro maiores desafios encontrados podem ser sumarizados em dois: (i) as informações recebidas são relevantes, confiáveis, revisadas e corroboradas, contribuindo com os componentes dos controles internos *(ICOFR)*; e (ii) os riscos futuros são discutidos com profundidade com o Conselho de Administração e o Comitê de Auditoria. No primeiro tópico, para que a Administração tenha êxito, perguntas-chave que devem ser feitas são:

- Que tipo de informação o Conselho de Administração/o Comitê de Auditoria/os Executivos recebem?
- Esta informação é completa e precisa para que o Conselho de Administração/o Comitê de Auditoria/os Executivospossam analisar detalhadamente e apresentar visões alternativas?

Com resposta a essas perguntas estamos pontuando não somente que as reuniões periódicas, como do Conselho e do Comitê, devem ser detalhadas em *minutes meetings* compreensíveis, indicando as discussões realizadas, as questões levantadas, as decisões tomadas e os próximos passos ou ações a serem aplicadas, mas também que relatórios-chave usados pelo Conselho de Administração, o Comitê de Auditoria e os Executivos devem ser criados, mantidos, corroborados e atualizados, contribuindo com a geração de uma informação completa e precisa para um *oversight* pontual e assertivo.

No segundo tópico, o Conselho de Administração e o Comitê de Auditoria assumem a responsabilidade pela supervisão da elaboração, da introdução e da execução dos controles internos pela Administração e, deste modo, pelo menos em bases anuais, o Conselho de Administração e o Comitê de Auditoria têm um *fresh look* dos riscos futuros que possam impactar a Empresa no atingimento do *Internal Control Over Financial Reporting (ICOFR)*, considerando discussões evidenciadas em detalhadas atas de reunião sobre: novos mercados, mudanças regulatórias, mudanças de lideranças dentro da Empresa, transações significativas (ex.: reestruturação de negócios), processos com "oportunidades"de ocorrer fraudes (ex.: utilização/eliminação de sucata) etc. O Conselho de Administração e o Comitê de Auditoria devem ser informados sobre como os riscos são identificados, avaliados e respondidos no nível de entidade e processos - vide comentários adicionais na resposta aos princípios 7, 8 e 9.

Questão 3

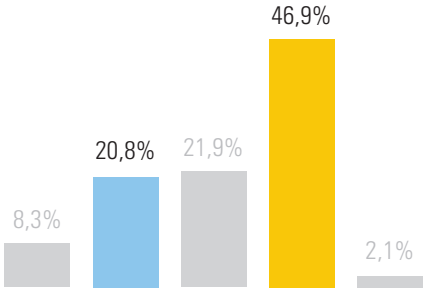
Qual seria o desafio para adotarmos/implementarmos o princípio 3 em nossas Empresas?

Evidenciar a supervisão efetiva da Administração sobre as obrigações e os trabalhos (assignments) realizados pelos subcontratados/terceirizados.

46,9%

Estruturar canais de comunicação, formais e independentes, que realmente possibilitem a prestação de contas, tempestiva, dos subcontratados/terceirizados.

20,8%

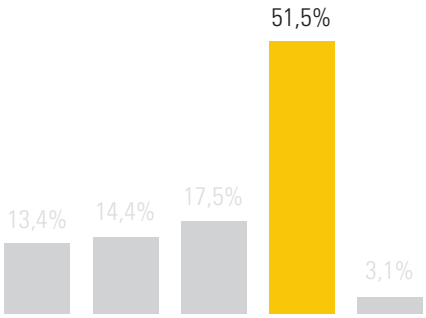


Questão 4

Qual seria o desafio para adotarmos/implementarmos o princípio 4 em nossas Empresas?

Documentar a avaliação da competência (habilidades e conhecimentos) dos subcontratados/terceiros da Empresa.

51,5%



Princípio 3: A Administração estabelece, com supervisão do Conselho de Administração, estruturas, quem responde para quem e os poderes e as responsabilidades adequados para a busca dos objetivos.

Princípio 4: A organização demonstra comprometimento com a atração, o desenvolvimento e a retenção de indivíduos competentes em harmonia com os objetivos.

O princípio 3 — "A Administração estabelece, com supervisão do Conselho de Administração, estruturas, quem responde para quem e os poderes e as responsabilidades adequados para a busca dos objetivos" — é focado em: (i) as *reporting lines* e os canais de comunicação devem ser "claros" para possibilitar a prestação de contas pelas unidades, pelas áreas e por *outsourced service provider*; (ii) a Administração deve supervisionar (*oversee*) a definição e a limitação das responsabilidades, das obrigações e do trabalho (*assignment*) para os executivos; e (iii) a segregação de funções deve ser considerada em todos os níveis da organização.

Já o princípio 4 — "A organização demonstra comprometimento com a atração, o desenvolvimento e a retenção de indivíduos competentes em harmonia com os objetivos" — tem como *main target* a existência de avaliações periódicas para garantir habilidades e conhecimentos dentro da Empresa.

Entretanto, nos dois princípios, o resultado da pesquisa interativa efetuada indicou atenção ao tópico subcontratados/terceirizados, sendo: (a) "Evidenciar a supervisão efetiva da Administração sobre as obrigações e os trabalhos (*assignments*) realizados pelos subcontratados/terceirizados; (b) "Estruturar canais de comunicação, formais e independentes, que realmente possibilitem a prestação de contas, tempestiva, dos subcontratados/terceirizados"; e (c) "Documentar a avaliação da competência (habilidades e conhecimentos) dos subcontratados/terceiros da Empresa".

A Estrutura Integrada COSO 2013 foca em todos os níveis da entidade no princípio 1, sendo a entidade definida como o grupo ou a corporação, bem como suas subsidiárias, divisões, unidades funcionais e departamentos dentro da Empresa.Todavia, o que é interessante é que o COSO 2013 vai além do tradicional entendimento de entidade (citado acima), incluindo como *extented business model* os subcontratados, parceiros de negócios e outros parceiros externos da Empresa. Logo, na avaliação da efetividade do *ICOFR* da Empresa a Alta Administração deve avaliar seus subcontratados e seus parceiros de negócio tempestivamente, mesmo confiando em seus serviços, pois a Administração detém a responsabilidade sobre a efetividade de seus controles internos — totalmente consistente com o *SEC´s* 2007 *Interpretive Guidance on Management´s Reporton ICOFR*. Essa avaliação deve levar em consideração:(i) a relação de controles internos que contribuam com o envio de 100% das informações aos subcontratados, para ajudar a garantir que o *input* das informações seja completo; (ii) a relação de controles internos, tal como *Management Review Controls (MRC)*, que contribuam com uma análise detalhada dos *outputs* recebidos dos subcontratados, ajudando a garantir erros toleráveis (precisão) e suporte documental apropriado (evidências nas revisões); (iii) os controles internos existentes durante o processamento das informações pelos terceiros, por exemplo *ISAE Report*; e (iv) os controles de monitoramento sobre a performance dos trabalhos realizados pelos subcontratados, por exemplo quantidade de reprocessamento de *outputs*, quantidade de ajustes retroativos em *outputs* passados, tempo de retorno para questionamentos da Empresa quanto à exatidão dos *outputs* gerados etc.

Questão 5

Qual seria o desafio para adotarmos/implementarmos o princípio 5 em nossas Empresas?

Definição, pela Empresa, de "mecanismos" (processos formais) para acompanhar seus empregados na execução efetiva de suas responsabilidades advindas do *ICOFR*.

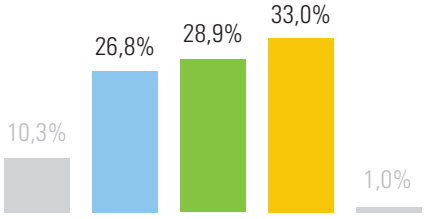
33%

Definição, pela Empresa, de regras do programa de incentivo aos funcionários (PLR) "balanceadas" entre objetivos/metas de curto e longo prazos — none excessive pressure.

28,9%

Definição, pela Empresa, de regras do programa de incentivo aos funcionários (PLR) "balanceadas" entre medições financeiras (ex.: vendas) e não financeiras (ex.: conduta de ética).

26,8%



Princípio 5: A organização responsabiliza os indivíduos pelos controles internos a eles atribuídos para a busca dos objetivos.

Neste princípio,o que destacamos é que "falta de 'pressão' pode resultar em *performance* baixa e que muita 'pressão' pode gerar *circumvent processes/ override controls* (transgressão de controles internos) ou encorajar atividades fraudulentas". Logo, encontrar o balanço correto é a questão-chave e há necessidade de possuirmos mecanismos que contribuam para que o ambiente de controle da Empresa esteja presente (em relação ao desenho do controle interno) e em funcionamento (em relação à efetividade do controle interno) no tocante ao *ICOFR*.

De acordo com o Controle Interno sobre Reporte Financeiro Externo: Um Resumo de Abordagens e Exemplos do COSO 2013, uma forma de referência seria a avaliação periódica e formal de uma análise imparcial dos incentivos e dos programas de premiação alcançados pelos gestores e pelos empregados. Em alguns casos (ex.: no caso de executivos), os resultados das avaliações seriam reportados ao Conselho de Administração e ao Comitê de Auditoria.

Em suma, para auxiliar na avaliação do ambiente de controle em relação ao princípio 5, sugerimos que as seguintes perguntas sejam aplicadas e os resultados, evidenciados e/ou documentados:

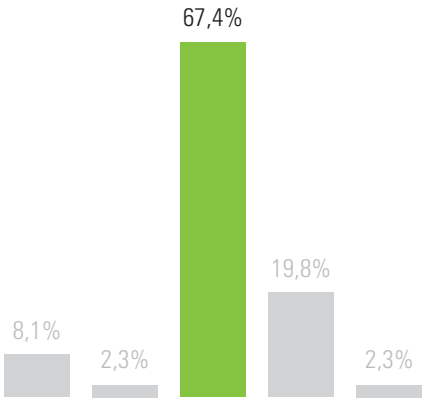
- Como a Empresa encoraja seus empregados a executar efetivamente as responsabilidades advindas do *ICOFR*?
- Quais são os mecanismos *in place*?
- O programa de incentivo aos funcionários (PLR) considera a responsabilidade dos funcionários sobre os controles internos?
- A Empresa, na definição das regras do programa de incentivo aos funcionários (PLR), considera o mix entre medições financeiras (ex.: vendas) e não financeiras (ex.: conduta ética)?
- Há um adequado "balanço" entre objetivos/metas de curto e longo prazos nas regras do programa de incentivo aos funcionários (PLR) —*none excessive pressure?*

Questão 6

Qual seria o desafio para adotarmos/implementarmos o princípio 6 em nossas Empresas?

Definir o risco de tolerância (precisão) dos controles internos.

67,4%

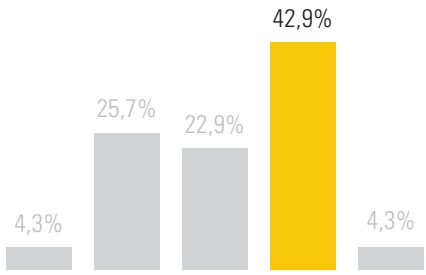


Questão 12

Qual seria o desafio para adotarmos/implementarmos o princípio 12 em nossas Empresas?

Definir o nível de precisão na execução da revisão gerencial.

42,9%



Princípio 6: A organização especifica objetivos com suficiente clareza a fim de possibilitar a identificação e a avaliação dos riscos relacionados aos seus objetivos.

Na pesquisa interativa efetuada no evento "Praticando o COSO 2013 - Estrutura Integrada", as questões 6 e 12, relativas aos princípios de mesmos números, destacaram a preocupação quanto à definição dos erros de tolerância (precisão) dos controles internos, sendo incluído o de natureza "revisão gerencial".

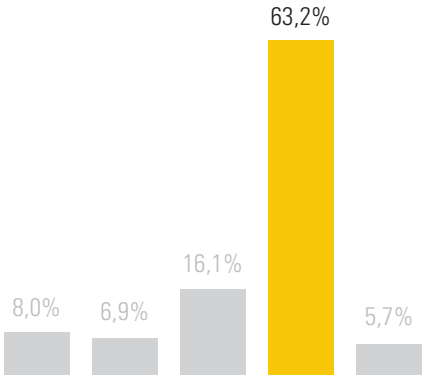
Lembramos que o erro de tolerância dos controles internos depende da habilidade em desenvolver precisas expectativas para identificar/pontuar potenciais erros materiais nas demonstrações financeiras para atendimento do *ICOFR*, bem como que o erro de tolerância nunca pode exceder a materialidade e é sempre significativamente inferior a essa materialidade. Dito isto, pense no controle *three-way match* no processo de compras como exemplo: suponhamos que o controle aceita desvios entre a fatura, o pedido de compra e o recebimento físico (documento) de R$100,00 e que estes R$100,00 representam o erro de tolerância (precisão) do desenho do controle *three-way match*. Se os R$100,00 são aceitos pelo funcionário/gestor milhares de vezes, eventualmente podemos ter um impacto significante nas demonstrações financeiras da Empresa. Logo, o erro de tolerância (precisão) deve combinar controles preventivos, detectivos e corretivos, os quais auxiliam a "balancear" impacto versus probabilidade — no caso do exemplo, *three-way match*, impacto (R$100,00) e probabilidade (20 recebimentos ao mês sem justificativa e, acima disso, aprovação de funcionário superior).

Questão 7

Qual seria o desafio para adotarmos/implementarmos o princípio 7 em nossas Empresas?

Documentar o processo de identificação, avaliação e resposta aos riscos que afetam os objetivos de *ICOFR* da Empresa.

63,2%

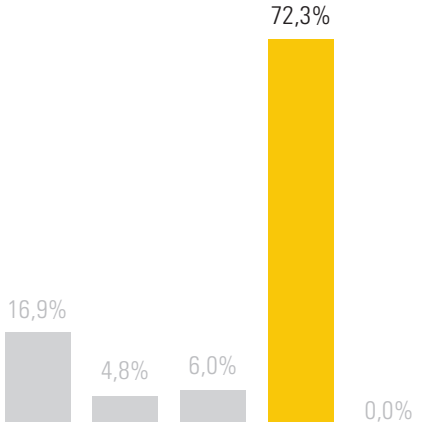


Questão 8

Qual seria o desafio para adotarmos/implementarmos o princípio 8 em nossas Empresas?

Documentar o processo de identificação, avaliação e resposta aos riscos potenciais de fraude que possam afetar os objetivos de *ICOFR* da Empresa.

72,3%

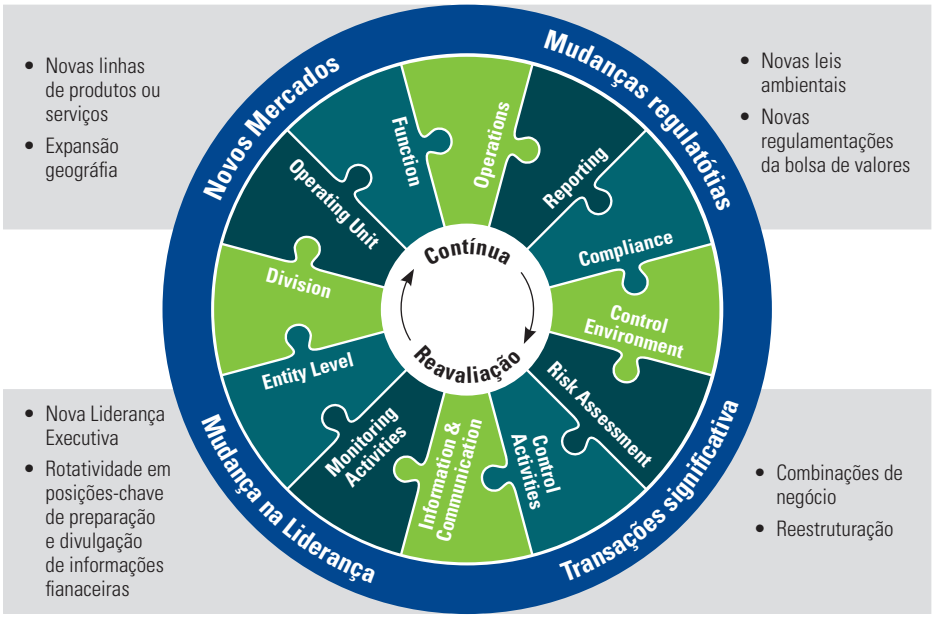


Princípio 7: A organização identifica riscos para a realização de seus objetivos e analisa riscos como uma base para determinar como os riscos deveriam ser gerenciados.

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

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

Os princípios 7, 8 e 9 estão relacionados ao componente Avaliação de Riscos. Cada um deles tem um enfoque, sendo, respectivamente: objetivos da entidade, potencial de fraude e ambiente de controle interno. Todavia, os três têm em comum os seguintes pontos: identificar, analisar e responder ao risco. O princípio 7 — "A organização identifica riscos para a realização de seus objetivos e analisa riscos como uma base para determinar como os riscos deveriam ser gerenciados" — foca em identificar, avaliar e responder aos riscos funcionais, de entidade, de subsidiária, de divisão e de unidade operacional, tendo como vertentes: novos mercados, mudanças regulatórias, mudanças de lideranças e transações significativas (vide painel 1).



Já o princípio 8 — "A organização considera o potencial de fraude na avaliação de riscos para o alcance dos objetivos" — visa à identificação, à análise e à resposta para impedir ou detectar oportunamente uma omissão ou uma divulgação distorcida significativa das demonstrações financeiras devido a erro ou fraude, atentando para: "oportunidades" para fraudes, incentivos e pressões ("referenciado" ao princípio 5) e falta de ética (vide painel 2).

Tipos de fraude:

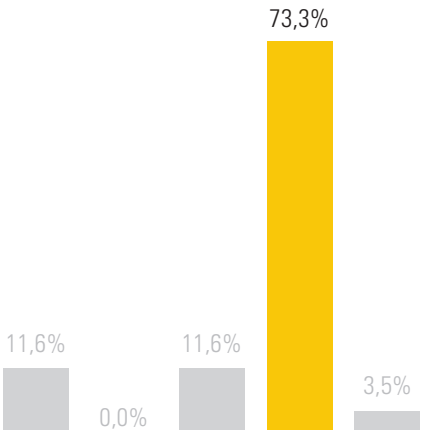
- Preparação e divulgação fraudulenta de informações financeiras
- Desvio de ativos
- Corrupção e outros atos ilegais
- Transgressão dos controles internos por partes da Administração

Questão 9

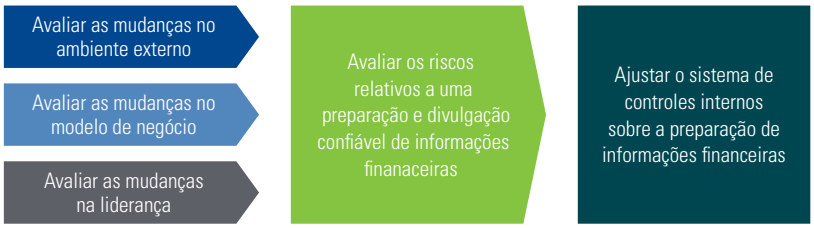
Qual seria o desafio para adotarmos/implementarmos o princípio 9 em nossas Empresas?

Documentar o processo de identificação, avaliação e resposta às possíveis mudanças no ambiente de controles que possam afetar objetivos de *ICOFR* da Empresa.

73,3%



Por último, mas não menos importante, o princípio 9 dita que "A organização identifica e avalia mudanças que poderiam impactar significativamente o sistema de controle interno", por meio da sinalização de sistemas de alerta precoce que devem ser instalados para identificar as informações que sinalizam novos riscos que possam ter um impacto significativo sobre a entidade (vide painel 3).



O resultado da pesquisa interativa efetuada indicou a preocupação dos participantes em como "documentar o processo de identificação, avaliação e resposta aos riscos: (i) que afetam os objetivos de *ICOFR* da Empresa; (ii) de potenciais de fraude que possam afetar objetivos de *ICOFR* da Empresa; e (iii) de possíveis mudanças no ambiente de controles que possam afetar os objetivos de *ICOFR* da Empresa"e, por conseguinte, sugerimos auxílio por meio do seguinte exemplo — foco no *ICOFR*:

A Administração reavalia a Avaliação de Riscos de acordo com as regras da SOX a cada ano:

1. Considera os riscos em vários níveis da organização, incluindo a entidade como um todo, subunidades e processos. Os riscos de prestadores de serviço terceirizados são também considerados.

2. Considera os fatores quantitativos (ex.: materialidade) e qualitativos, tais como:
   - Riscos econômicos
   - Riscos do ambiente natural
   - Riscos regulatórios
   - Mudanças na estrutura e na infraestrutura da Administração
   - Nível e competência dos funcionários
   - Riscos de fraude — a possibilidade de acesso dos funcionários aos ativos pode aumentar o risco de desvio de recursos

Os riscos são identificados para transações nos processos de negócio, subsidiárias, funções e unidades operacionais. Determinam quais rubricas das demonstrações financeiras serão incluídas no escopo do programa de conformidade com as regras da SOX por meio da aplicação de um nível de materialidade calculado de maneira sistemática e da consideração de outros fatores de risco, tais como:

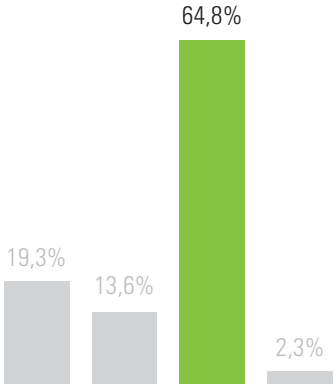
- A competência dos funcionários
- O nível da estimativa e da complexidade
- O potencial de transgressão e de existência de um viés da Administração
- O nível de transações não rotineiras/manuais versus as transações rotineiras e sistemáticas
- O nível de deficiências de controle passadas
- O risco de fraude
- A centralização *versus* a descentralização das atividades de controle
- A localização das atividades de controle, como localizações remotas.

Questão 10

Qual seria o desafio para adotarmos/implementarmos o princípio 10 em nossas Empresas?

Categorizar os Controles-chave em Nível de Transação (Transactional-Level Controls) em alto, médio ou baixo, considerando sua dependência de informações advindas de relatórios gerados via *query* ou planilhas eletrônicas.

64,8%



Princípio 10: A organização seleciona e desenvolve atividades de controle que contribuem para a mitigação de riscos em níveis aceitáveis para a realização dos objetivos.

O princípio 10 endereça como selecionam-se e desenvolvem-se os controles internos que contribuem ou mitigam os riscos da Empresa no atingimento de seus objetivos — a um nível aceitável de risco. O termo "um nível aceitável de riscos" refere-se ao erro tolerável (precisão), o qual é identificado e reconhecido pela Empresa como um balizador para que os controles internos auxiliem com razoabilidade, mas não absoluta certeza, que os objetivos podem ser atingidos. Na pesquisa interativa, realizada em 12 de março de 2015, os participantes externaram preocupação quanto ao "Categorizar os Controles-chave em Nível de Transação *(Transactional-Level Controls)* em alto, médio ou baixo, considerando sua dependência de informações advindas de relatórios gerados via *query* ou planilhas eletrônicas". Lembramos que a categorização de relatórios gerados via *query*, chamados de *Information Provided by the Entity (IPE)*, ou via planilhas eletrônicas,chamadas de *End-User Computing (EUC)*, deve ponderar a função de IPE ou EUC—se simples (ex.: somente compilação de dados "somados") ou complexas (cálculos elaborados por macros).Deste modo, costumamos considerar em nossas avaliações:

- Complexidade e cálculos da planilha
- Propósito e uso da planilha
- Número de usuários da planilha, incluindo sua segurança
- Tipo de entrada de dados, lógica e erros de interface
- Tamanho da planilha
- Nível de entendimento do desenvolvedor
- Qualidade da documentação da planilha efetuada pelo desenvolvedor
- Uso de informações de saída da planilha
- Frequência e extensão de mudanças na planilha
- Desenvolvimento, desenvolvedor (incluindo treinamento) e testes da planilha antes de ser utilizada.

Questão 11

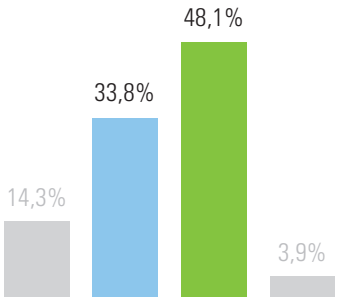
Qual seria o desafio para adotarmos/implementarmos o princípio 11 em nossas Empresas?

Documentar a efetividade dos Controles Automatizados e dos Controles Gerais de Tecnologia da Informação que respaldam as operações.

48,1%

Vincular os Controles Automatizados, no Nível dos Processos, com os Controles Gerais de Tecnologia da Informação que respaldam as operações.

33,8%



Princípio 11: A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para respaldar a consecução dos objetivos.

Em termos de Controles de Tecnologia da Informação, enfoque do princípio acima, a Administração entende e determina a dependência e o uso da tecnologia nos seus processos de negócio, bem como identifica sua necessidade por Controles Gerais de Tecnologia da Informação (GITC) para suportar suas operações consistentemente. Logo, conforme indicado pelas respostas à pergunta interativa, os desafios estão em: "Documentar a efetividade dos Controles Automatizados e dos Controles Gerais de Tecnologia da Informação que respaldam as operações" e "Vincular os Controles Automatizados, no Nível dos Processos, com os Controles Gerais de Tecnologia da Informação que respaldam as operações".

Em relação a "vincular os controles automatizados", quando a Administração entende sua dependência e seu uso da tecnologia nos seus processos de negócio, a Empresa compreende o fluxo das informações financeiras referentes a cada processo, iniciando do "último uso" (ex.: apresentação das demonstrações financeiras) e percorrendo o processo de "coleta das informações" atentando para riscos e controles internos, incluindo aplicativos.

A título de exemplo, vamos considerar um controle que confiamos como um *system-enforced segregation of duties* entre funções incompatíveis, tais como funcionário registrando um fornecedor (atualizado o cadastro de fornecedores) e os funcionários iniciando e aprovando pedidos de compra, que são endereçadas ao risco de utilização indevida de fundos da Empresa. Pontuamos, neste caso, o risco de o controle não ser consistente e ocasionar a falha do *system-enforced segregation of duties*— vinculamos o controle automatizado no nível dos processos (o de segregação de função) aos controles gerais de tecnologia da informação potencialmente relevantes, que são, neste caso, os seguintes: controles sobre o provisionamento dos usuários; controles sobre a revisão periódica do acesso dos usuários; e controles sobre o acesso privilegiado de usuários.

Em relação a "documentar a efetividade dos controles automatizados", entendemos que o melhor modo de explicar é exemplificando: recentemente, temos observado uma maior utilização de End-User Computing (EUC), o qual, se automático ou manual, é categorizado como aplicativo. Deste modo, o EUC necessita ser entendido, documentado e controlado, ou seja, os sistemas de desenvolvimento, as mudanças de programas e os controles de acesso sobre as planilhas precisam ser formalmente entendidos e documentados (ex.: políticas de planilhas eletrônicas e roteiro para a avaliação de planilhas eletrônicas).

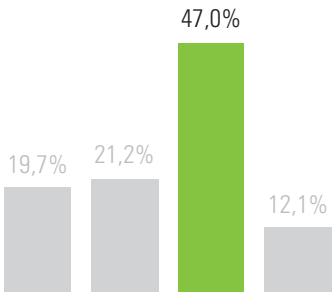
De maneira resumida, ambas as respostas apontam para desafios que as corporações encontram para mapear adequadamente o contexto de negócios (seus processos, produtos e serviços) e os sistemas aplicativos que suportam as suas operações, seus controles e o fluxo de dados para a geração das informações que compõem as demonstrações financeiras. O adequado mapeamento do contexto de negócio permite que se identifique o escopo completo de análise, as sinergias entre os controles e seus testes, e a documentação de maneira consistente e assertiva da efetividade dos controles.

Questão 14

Qual seria o desafio para adotarmos/implementarmos o princípio 14 em nossas Empresas?

Definir o público-alvo interno da Empresa que deve receber as comunicações para suportar os componentes dos controles internos *(ICOFR)*.

47%

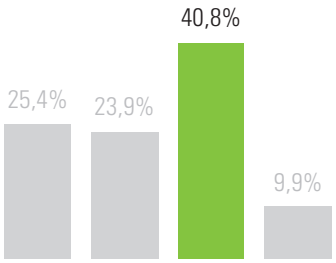


Question 15

Qual seria o desafio para adotarmos/implementarmos o princípio 15 em nossas Empresas?

Definir o público-alvo externo da Empresa que deve receber as comunicações sobre o funcionamento dos seus componentes dos controles internos *(ICOFR)*.

40,8%



Princípio 14: A organização comunica informações internamente, incluindo objetivos e responsabilidades para controle interno, necessários para suportar o funcionamento de outros componentes de controle interno.

Em relação ao princípio 14, o COSO 2013 endereça como a informação é comunicada internamente, sendo a comunicação focada em oral (ex.: *workshops*) e escrita, canais normais ou anônimos/confidenciais (ex.: *whistleblower*). Ademais, a Estrutura Integrada pontua que comunicação diretamente relevante para contribuir com a efetividade dos controles internos pode requerer a aplicação de uma metodologia de retenção de documentos (*long-term retention*, conforme descrito no COSO 2013), bem como que comunicações sensíveis, mas que não requerem confidencialidade ou retenção, podem ser feitas por *e-mail*, mensagens de texto e mídia social (podem ser suficientes a um custo-benefício aceitável).

Já o princípio 15 também segue a "mesma direção", mas foca em como a informação é comunicada externamente.

Na pesquisa interativa, o desafio foi pontuado em como "definir o público-alvo: interno e externo da empesa".

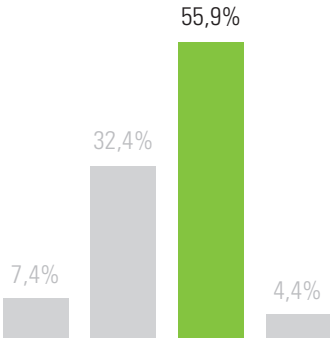
Logo, em relação ao público-alvo interno, o princípio 14 foca em como é feita a comunicação de informações aos Executivos, ao Conselho de Administração, ao Comitê de Auditoria e aos outros profissionais para possibilitar que estes sejam responsáveis pelos controles internos. Enquanto isso, o público-alvo externo coberto pelo princípio 15 são as comunicações recebidas e enviadas para terceiros (subcontratados), mercado (ex.: bolsa de valores), executivos, Conselho de Administração e Comitê de Auditoria.

Question 16

Qual seria o desafio para adotarmos/implementarmos o princípio 16 em nossas Empresas?

Desenhar os relatórios de avaliações específicas que podem antecipar mudanças nos processos (ex.: elevação na quantidade de produtos em estoque próximo da data de expiração), auxiliando na detecção e/ou na correção de erros nas demonstrações financeiras.

55,9%



Princípio 16: A organização seleciona, desenvolve e efetua avaliações contínuas e/ou específicas para determinar se os componentes de controle interno estão presentes e em funcionamento.

Este princípio esclarece a diferença entre atividades de controle e atividades de monitoramento, conforme apresentado a seguir:

Atividade de Controle	Atividade de Monitoramento
• Opera com precisão para abordar os riscos de afirmações específicas das demonstrações financeiras • Responde a riscos especificados (o que pode dar errado) • Designada para detector e corrigir erros nas afirmações das demonstrações financeiras	• Opera com precisão para abordar os riscos de afirmações específicas das demonstrações financeiras • Monitora a operação eficaz das Atividades de Controle • Monitora a correção de deficiências

As atividades de Monitoramento avaliam se os controles em cada um dos cinco componentes está operando conforme planejado

As atividades de Monitoramento NÃO substituem as Atividades de Controle, AMBAS são importantes

Além disso, o princípio 16 também requer que as Empresas selecionem, desenvolvam e realizem avaliações contínuas *(Ongoing Evaluation)* e avaliações separadas *(Separate Evaluations)* para "descobrir" se os componentes dos controles internos estão presentes e em funcionamento.

Na pergunta interativa, o desafio pontuado foi referente às avaliações contínuas. De acordo com a Estrutura Integrada COSO 2013, fluxogramas ou narrativos são o ponto de partida das avaliações contínuas, pois é neles que fazemos o entendimento dos processos, identificamos os riscos mais rapidamente e, portanto, podemos desenhar um relatório que possa detectar o "erro" na sua origem - *root cause*.

Question 17

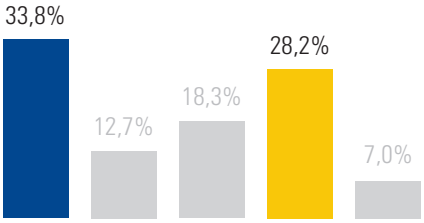
Qual seria o desafio para adotarmos/implementarmos o princípio 17 em nossas Empresas?

Dificuldade em determinar a root cause da deficiência

33,8

Dificuldade em identificar controles compensatórios

28,2



Princípio 17: A organização avalia e comunica deficiências de controle interno de maneira tempestiva para as partes responsáveis pela tomada de medidas corretivas, incluindo Alta Administração, quando apropriado.

Por último, e não menos importante, o princípio 17 dá foco na avaliação das deficiências nos controles internos, áreas que mais estão atraindo a atenção da *SEC* e do *PCAOB*. Este princípio lista os seis passos para a Alta Administração da Empresa avaliar suas deficiências e, de acordo com a pesquisa interativa, os desafios estariam nos passos 2 e 3 (dificuldade em determinar a *root cause* da deficiência) e nos passos 5 e 6 (dificuldade em identificar controles compensatórios). Em relação aos passos 2 e 3, com frequência observamos as Empresas focarem suas análises no erro financeiro e não na deficiência do controle interno que, quando falho, não contribui com a detecção ou a prevenção de um erro. Logo, um modo de identificar *root causes* é por meio da aplicação das seguintes questões:

- Qual é a deficiência de controle?
- Quais outras deficiências de controle podem existir relacionadas a este operador de contas/controles?
- O controle estava operando de maneira ineficaz — uma questão de monitoramento?
- O controle não foi elaborado de maneira adequada — uma questão de avaliação de risco?
- O operador dos controles tinha conhecimento suficiente — uma questão de ambiente de controle?
- O operador dos controles tinha informações incorretas — uma questão de informações e comunicação?

Quanto aos passos 5 e 6, lembramos que controles compensatórios devem ser considerados quando avaliamos a severidade de uma deficiência ou combinação de deficiências.Deste modo, o caminho para a identificação de controles compensatórios é feito no nível de processos/operações, pontuando o nível de precisão deste controle compensatório em prevenir ou detectar erros materiais nas demonstrações financeiras intermediárias e anuais.

kpmg.com/BR

 / kpmgbrasil

App KPMG Brasil – disponível em iOS e Android
App KPMG Publicações – disponível em iOS e Android