**ANEXO I – ESTRUTURA COSO ICIF 2013**

Os componentes, princípios e pontos de foco estabelecidos no framework COSO ICIF 2013 servem como referência para a avaliação dos controles internos do objeto de auditoria. O Quadro a seguir apresenta os componentes do controle interno, os princípios e os pontos de foco relacionados a eles.

Quadro 1

| **Componente do Controle Interno** | **Princípios relacionados** | **Pontos de Foco** |
| --- | --- | --- |
| **AMBIENTE DE CONTROLE**  O ambiente de controle representa um conjunto de normas, de processos e de estruturas que fornece a base para a aplicação do controle interno em toda a organização. A estrutura de governança e a alta administração ditam o exemplo de liderança a ser seguido, em relação à importância do controle interno e às normas de conduta esperadas. | 1) A organização demonstra ter comprometimento com a integridade e os valores éticos. | * Liderar pelo exemplo. * Estabelecer normas de conduta. * Avaliar a adesão às normas de conduta. * Tratar desvios de forma oportuna. |
| 2) A estrutura de governança demonstra independência em relação aos seus executivos e supervisiona o desenvolvimento e o desempenho do controle interno | * Estabelecer as responsabilidades pela supervisão. * Utilizar experiências relevantes. * Operar de forma independente. * Exercer a supervisão do sistema de controle interno: ambiente de controle; avaliação de riscos; atividades de controle; informação e comunicação; atividades de monitoramento. |
| 3) A administração estabelece, com a supervisão da estrutura de governança, as estruturas, os níveis de subordinação e as autoridades e responsabilidades adequadas para a busca dos objetivos. | * Considerar todas as estruturas da entidade. * Estabelecer linhas de subordinação. * Definir, atribuir e limitar autoridades e responsabilidades (estrutura de governança, alta administração, administração, pessoal, prestadores de serviços terceirizados). |
| 4) A organização demonstra comprometimento para atrair, desenvolver e reter talentos competentes em linha com seus objetivos. | * Estabelecer políticas e práticas. * Avaliar a competência e tratar as deficiências. * Atrair, reter e desenvolver talentos. * Planejar e preparar a sucessão |
| 5) A organização faz com que as pessoas assumam responsabilidades por suas funções de controle interno na busca pelos objetivos | * Exigir a prestação de contas, por meio de estruturas, autoridades e responsabilidades. * Estabelecer métricas, incentivos e recompensas de desempenho. * Avaliar continuamente a relevância de métricas, incentivos e recompensas de desempenho. * Considerar pressões excessivas. * Avaliar o desempenho e recompensar ou disciplinar as pessoas |
| **AVALIAÇÃO DE RISCOS**  A avaliação de riscos envolve um processo dinâmico e iterativo para identificar e analisar os riscos à realização dos objetivos da entidade. Essa avaliação constitui a base para determinar como esses riscos devem ser gerenciados. A administração leva em conta possíveis mudanças no ambiente externo e no seu próprio modelo de negócio que podem interferir em sua capacidade de realizar os objetivos. | 6) A organização especifica os objetivos com clareza suficiente para permitir a identificação e a avaliação dos riscos associados aos objetivos. | **Objetivos operacionais**   * Refletir as escolhas da administração. * Considerar as tolerâncias ao risco. * Incluir metas de desempenho operacionais e financeiras. * Formar uma base para o comprometimento de recursos.   **Objetivos de divulgação financeira externa:**   * Estar em conformidade com as normas de contabilidade aplicáveis. * Considerar a materialidade. * Refletir as atividades da entidade.   **Objetivos de divulgação financeira externa:**   * Estar em conformidade com as normas e as estruturas estabelecidas externamente. * Considerar os níveis exigidos de precisão. * Refletir as atividades da entidade.   **Objetivos de divulgação interna:**   * Refletir as escolhas da administração. * Considerar o nível exigido de precisão. * Refletir as atividades da entidade.   **Objetivos de conformidade:**   * Refletir leis e regulamentos externos. * Considerar as tolerâncias ao risco. |
| 7) A organização identifica os riscos à realização de seus objetivos por toda a entidade e analisa os riscos para determinar a forma como devem ser gerenciados. | * Incluir os níveis de entidade, subsidiária, divisão, unidade operacional e áreas funcionais. * Analisar fatores internos e externos. * Envolver os níveis apropriados da administração. * Estimar a importância dos riscos identificados. * Determinar como responder aos riscos |
| 8) A organização considera o potencial para fraude na avaliação dos riscos à realização dos objetivos. | * Considerar os vários tipos de fraude. * Avaliar incentivos e pressões. * Avaliar oportunidades. * Avaliar atitudes e racionalizações. |
| 9) A organização identifica e avalia as mudanças que poderiam afetar, de forma significativa, o sistema de controle interno. | * Avaliar as mudanças no ambiente externo. * Avaliar as mudanças no modelo de negócios. * Avaliar mudanças na liderança |
| **ATIVIDADES DE CONTROLE**  As atividades de controle são ações estabelecidas por meio de políticas e procedimentos, que ajudam a assegurar que as diretrizes da administração para mitigar os riscos à realização dos objetivos sejam cumpridas. As atividades de controle são realizadas em todos os níveis da entidade e em vários estágios dos processos corporativos, assim como no ambiente de tecnologia. | 10) A organização seleciona e desenvolve atividades de controle que contribuem para a redução, a níveis aceitáveis, dos riscos à realização dos objetivos. | * Integrar-se com a avaliação de riscos. * Considerar fatores específicos à entidade. * Determinar os processos de negócios relevantes. * Avaliar a combinação de tipos de atividades de controle. * Considerar em quais níveis as atividades são realizadas. * Abordar a segregação de funções |
| 11) A organização seleciona e desenvolve atividades de controle gerais sobre a tecnologia para apoiar a realização dos objetivos. | * Determinar a dependência entre o uso da tecnologia nos processos de negócios e os controles gerais de tecnologia. * Estabelecer atividades de controle sobre a infraestrutura da tecnologia relevante. * Estabelecer atividades de controle sobre os processos relevantes de gerenciamento de segurança. * Estabelecer atividades de controle sobre os processos relevantes de aquisição, desenvolvimento e manutenção de tecnologia. |
| 12) A organização estabelece atividades de controle por meio de políticas que estabelecem o que é esperado e os procedimentos que colocam em prática essas políticas | * Estabelecer políticas e procedimentos para apoiar a implementação das diretrizes da administração. * Estabelecer responsabilidade e prestação de contas pela execução das políticas e procedimentos. * Realizar tempestivamente. * Tomar decisões corretivas. * Realizar recorrendo a pessoal competente. * Reavaliar políticas e procedimentos. |
| **INFORMAÇÃO E COMUNICAÇÃO**  As informações são necessárias para que a entidade cumpra as responsabilidades de controle interno visando apoiar a realização de seus objetivos. A comunicação ocorre tanto interna quanto externamente e fornece à organização as informações necessárias para conduzir os controles do dia a dia. A comunicação permite que os funcionários compreendam as responsabilidades de controle interno e sua importância para a realização dos objetivos. | 13) A organização obtém ou gera e utiliza informações significativas e de qualidade para apoiar o funcionamento do controle interno. | * Identificar os requisitos de informações. * Capturar fontes internas e externas de dados * Processar dados relevantes em informações. * Manter a qualidade durante todo o processamento. * Considerar custos e benefícios. |
| 14) A organização transmite internamente as informações necessárias para apoiar o funcionamento do controle interno, inclusive os objetivos e as responsabilidades pelo controle interno. | * Comunicar as informações de controle interno. * Comunicar-se com a estrutura de governança. * Fornecer linhas de comunicação independentes. * Selecionar métodos de comunicação relevantes. |
| 15) A organização comunica-se com os públicos externos sobre assuntos que afetam o funcionamento do controle interno. | * Comunicar-se com públicos externos. * Possibilitar o recebimento de comunicações. * Comunicar-se com a estrutura de governança. * Fornecer linhas de comunicação independentes. * Selecionar métodos de comunicação relevantes. |
| **MONITORAMENTO**  Avaliações contínuas, independentes, ou alguma combinação dessas duas são utilizadas para garantir que cada um dos cinco componentes de controle interno, inclusive os controles para colocar em prática os princípios de cada componente, está presente e funcionando. Os resultados são avaliados e as deficiências são comunicadas em tempo hábil, sendo que as questões graves são relatadas à estrutura de governança e à alta administração. | 16) A organização seleciona, desenvolve e realiza avaliações contínuas e/ou independentes para se certificar da presença e do funcionamento dos componentes de controle interno. | * Considerar uma combinação de avaliações contínuas e independentes. * Considerar o ritmo das mudanças. * Estabelecer o entendimento da base de referência. * Utilizar pessoal com conhecimento. * Integrar aos processos de negócios. * Ajustar o escopo e a frequência. * Avaliar objetivamente. |
|  | 17) A organização avalia e comunica deficiências no controle interno em tempo hábil aos responsáveis por tomar ações corretivas, inclusive à estrutura de governança e à alta administração, conforme aplicável. | * Avaliar resultados. * Comunicar deficiências. * Monitorar as ações corretivas. |

Fonte: Ministério da Transparência e Controladoria-Geral da União **Orientação Prática: Relatório de Auditoria**. Brasília: CGU, 2019