The Institute of Internal Auditors Australia

Guia de Melhores Práticas de Auditoria Interna para Serviços Financeiros na Austrália

TRADUZIDO POR • INSTITUTO DOS AUDITORES INTERNOS DO BRASIL •

IA Brasil

Novembro de 2020

Conectar › Apoiar › Progredir

CONTEÚDOS

Prefácio 4

Mensagem da Presidente 5

Propósito e aplicação do guia de melhores práticas 6

PRINCÍPIO 1 7
Posicionar a auditoria interna para o sucesso

PRINCÍPIO 2
Garantir recursos e senioridade adequados 10

PRINCÍPIO 3
Prestar avaliação que agregue valor 13

PRINCÍPIO 4
Empregar métodos e ferramentas apropriadas à tarefa 16

PRINCÍPIO 5
Reportar para influenciar mudanças positivas 19

PRINCÍPIO 6
Adotar metodologias apropriadas para auditar a cultura de risco 22

ANEXOS

Anexo A
Modelos operacionais de auditoria interna 25

Anexo B
O Modelo das Três Linhas 26

Anexo C
Glossário de termos 27

Comitê de Serviços Financeiros do IIA 29

Sobre o Institute of Internal Auditors 30

PREFÁCIO

O Comitê para desenvolver orientações de melhores práticas de auditoria interna para o setor de serviços financeiros fez um excelente trabalho na formulação de um documento baseado em princípios. O Institute of Internal Auditors – Austrália aceitou todas as suas recomendações.

Estou confiante de que os Comitês de Auditoria e os profissionais de auditoria interna adotarão os princípios contidos no Guia de Melhores Práticas e os aplicarão com rigor e sem hesitação, para obter melhores resultados de governança para o setor.

O Comitê, presidido pela diretora não executiva Sandra Birkensleigh, era composto por auditores internos e membros de Comitês de Auditoria bancários, de previdência, seguros e da Academia.

Gostaria de agradecer ao Comitê e a seus membros em nome do Instituto pelo excelente trabalho que realizaram.

Este guia de auditoria interna delineia as atividades que devem ser conduzidas de forma consistente com o Framework Internacional de Práticas Profissionais (IPPF, incluindo os Princípios Fundamentais para a Prática Profissional de Auditoria Interna, a Definição de Auditoria Interna, o Código de Ética e as Normas Internacionais para a Prática Profissional de Auditoria Interna (’as *Normas’*)). O guia também complementará os Princípios e Recomendações do *ASX Corporate Governance Council* (4ª edição).

Por fim, gostaria de estender gratidão do IIA-Austrália pelo apoio de secretaria fornecido pela EY e pela KPMG, que foram fundamentais para garantir que a orientação fosse concluída de forma rápida e sem complicações.

Peter Jones
CEO, Institute of Internal Auditors – Austrália

Mensagem da Presidente

O setor de serviços financeiros australiano está sob maior escrutínio e pressão após a *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry*.

Como acontece com qualquer Comissão Real ou Inquérito Prudencial de nossos serviços bancários e financeiros, devemos aprender com os erros e reformar rapidamente políticas e procedimentos para atingir resultados mais eficazes para nossos clientes, stakeholders e acionistas.

Uma clara falha de política, que foi levantada no Inquérito Prudencial da APRA sobre o CBA, foi o papel que a auditoria interna poderia desempenhar nas estruturas de governança. Em muitos casos, os relatórios de auditoria foram simplesmente ignorados.

Há muitos outros exemplos de auditores internos sendo ignorados pela alta administração e pelos Comitês de Auditoria.

Quando a Comissão Real concluiu suas audiências, o Institute of Internal Auditors – Austrália, em resposta ao Relatório Final da Comissão, também revisou as lições dos escândalos bancários no Reino Unido em 2013.

O *Chartered Institute of Internal Auditors (UK)*, em resposta aos escândalos, desenvolveu um guia de auditoria interna para o setor de serviços financeiros, publicando a primeira edição do documento *Effective Internal Audit in Financial Services Sector* em 2013, e revisando-o em 2017.

Uma pesquisa sobre a eficácia da orientação foi realizada em 2015 e descobriu que, no geral, os orçamentos de auditoria interna, o número de funcionários, os níveis de senioridade e os níveis de treinamento aumentaram. Também houve linhas de reporte aprimoradas dos chefes de auditoria interna aos Presidentes dos Comitês de Auditoria e linhas de reporte secundário aos CEOs.

Do ponto de vista da Austrália, a orientação do Reino Unido fornece um plano valioso para o desenvolvimento de um guia de auditoria interna eficaz para o nosso setor de serviços financeiros, que tem seus próprios aspectos exclusivos.

Estou muito satisfeita com o nível de engajamento da indústria de serviços financeiros australiana no desenvolvimento de nosso próprio guia de auditoria interna.

O guia define o que se espera da auditoria interna, para que Conselhos, Comitês de Auditoria e reguladores possam definir suas expectativas.

Este guia de auditoria interna deve ser aplicado em conjunto com o Framework Internacional de Práticas Profissionais (IPPF) e as Normas Internacionais para a Prática Profissional de Auditoria Interna (*'Normas'*), as únicas normas universalmente aplicáveis para profissionais de auditoria interna.

Tenho o privilégio de liderar um grupo distinto de profissionais da indústria e um acadêmico experiente em governança de riscos para criar nossa própria orientação, que ajudará os profissionais de auditoria interna, a alta administração, os presidentes do Comitê de Auditoria e os stakeholders a atingir nosso objetivo de melhorar as estruturas de governança.

O Instituto empreendeu um amplo processo de consulta ao setor de serviços financeiros para atingir esse resultado. O objetivo desejado é melhorar os resultados da governança corporativa para o benefício de todas as partes envolvidas.

Ao fim deste documento, encorajo fortemente a adoção desta orientação, pois é responsabilidade dos Conselhos, dos auditores internos e da alta administração garantir que as melhores práticas da função de auditoria interna sejam alcançadas para o benefício dos clientes, stakeholders e acionistas da entidade.

Por fim, também gostaria de agradecer aos nossos observadores, em especial à ASIC e APRA por seu apoio, e à EY e KPMG pelo apoio de secretariado.

Sandra Birkensleigh
Novembro de 2020

Propósito e aplicação do Guia de Melhores Práticas

Essas recomendações estabelecem práticas de auditoria interna para entidades de serviços financeiros na Austrália. O Comitê reconhece, porém, que diferentes entidades podem legitimamente adotar práticas distintas, com base em uma série de fatores, incluindo porte, complexidade, história e cultura corporativa.

Por esse motivo, as recomendações contidas no Guia de Melhores Práticas de Auditoria Interna para Serviços Financeiros na Austrália ('Guia de Melhores Práticas') não são obrigatórias e não buscam prescrever as práticas de auditoria interna que uma entidade deve adotar.

Embora as recomendações se apliquem a entidades de serviços financeiros, uma vez que refletem uma visão contemporânea das práticas apropriadas de auditoria interna, outros órgãos podem considerá-las úteis na formulação de suas práticas.

As recomendações devem orientar os conselhos, comitês de auditoria e chefes executivos de auditoria (CAEs) no estabelecimento e operação de uma atividade de auditoria interna.

As referências ao CAE devem ser entendidas como se referindo a um funcionário sênior da organização, responsável pela gestão eficaz da atividade de auditoria interna.

O Chefe Executivo de Auditoria é responsável pelo desempenho geral da atividade de auditoria interna, incluindo a conformidade com as Normas e outros requisitos organizacionais.

Nos casos em que o CAE dependa de terceiros para realizar o trabalho (p. ex., um subordinado, uma filial ou um prestador de serviços), o CAE permanece responsável por esse desempenho.

A estrutura das recomendações

As recomendações buscam promover e são estruturadas em torno de seis princípios centrais:

Princípio 1 – Posicionar a auditoria interna para o sucesso

O propósito principal da auditoria interna deve ser auxiliar o Conselho e a alta administração a proteger os ativos, a reputação e a sustentabilidade da organização.

Princípio 2 – Garantir recursos e senioridade adequados

A composição, estrutura e acordos de remuneração da auditoria interna devem apoiar uma avaliação independente e eficaz.

Princípio 3 – Prestar avaliação que agregue valor

A auditoria interna deve ser eficaz e agregar valor ao atender às necessidades e expectativas de avaliação do Conselho e dos stakeholders.

Princípio 4 – Empregar métodos e ferramentas apropriadas à tarefa

A auditoria interna deve manter uma metodologia atualizada, assim como suas práticas subjacentes e ferramentas associadas, para aumentar sua eficácia.

Princípio 5 – Reportar para influenciar mudanças positivas

A auditoria interna deve causar mudanças positivas, oferecendo informações tempestivas, precisas e perspicazes para uso como base para a tomada de decisões com foco em riscos.

Princípio 6 – Adotar metodologias apropriadas para auditar a cultura de risco

A responsabilidade por definir a cultura de risco é do Conselho da organização. A gestão organizacional, então, tem a responsabilidade de conduzir essa cultura de risco através da organização, mensurando e reportando sobre a cultura de risco, e determinando ações para resolver quaisquer lacunas. Como uma função independente, a auditoria interna pode prestar avaliação independente sobre os processos de governança em torno da cultura e reporte de riscos, mas também uma visão independente da própria cultura de risco. A auditoria interna presta avaliação em relação à cultura de risco, tanto por meio de auditorias das "operações normais de negócios" e quanto por meio de auditorias mais amplas da cultura de risco.

Existem 32 recomendações específicas de aplicação geral destinadas a dar efeito a esses princípios. Há também comentários explicativos, com mais orientações sobre as recomendações.

Quando apropriado, é feita referência às Normas Internacionais para a Prática Profissional (IPPF) de Auditoria Interna aplicáveis, em vigor a partir de janeiro de 2017.

O Anexo A contém uma visão geral e explicação dos diversos modelos operacionais de auditoria interna utilizados nas organizações na Austrália.

O Anexo B oferece uma visão geral do Modelo de Três Linhas dos componentes do gerenciamento eficaz de riscos da organização.

O Anexo C é um glossário dos principais termos usados neste documento.

PRINCÍPIO 1

Posicionar a auditoria interna para o sucesso

O propósito principal da auditoria interna deve ser auxiliar o Conselho e a alta administração a proteger os ativos, a reputação e a sustentabilidade da organização.

Recomendação 1.1

O papel da auditoria interna deve ser articulado em um estatuto de auditoria interna que esteja publicamente disponível e estabeleça:

a. O propósito principal da auditoria interna; e

b. O mandato da auditoria interna.

Comentários:

O Presidente do Comitê de Auditoria deve ter a responsabilidade de aprovar e supervisionar a conformidade com o estatuto de auditoria interna.

O Conselho, os subcomitês (incluindo o Comitê de Auditoria) e a alta administração devem ter um papel definido de estabelecer o 'tom do topo' e apoiar a auditoria interna em cumprir com seu propósito, papel e mandato, enquanto promovem a aceitação da auditoria interna em toda a organização.

Em termos gerais, o mandato da auditoria interna deve abranger:

- Colaboração ativa com a gestão e o Conselho, para informar uma compreensão dos principais riscos da organização, cobertura e escopo da auditoria;
- Questionamento proativo da gerência executiva, para melhorar a eficácia da cultura de risco, governança, gerenciamento de riscos e principais controles internos;[1]
- Avaliação sobre se todos os riscos significantes são identificados e devidamente reportados pela administração e função de risco ao Conselho; e
- Determinação independente sobre se os controles internos são adequados, dados os principais riscos à organização.

Referências às Normas do IIA (IPPF):

1000 – Propósito, Autoridade e Responsabilidade

1 Consulte a Recomendação 1.4

Recomendação 1.2

O Chefe Executivo de Auditoria ou Chefe de Auditoria Interna[2] deve ter uma linha de reporte primário ao Presidente do Comitê de Auditoria. Também pode haver uma linha de reporte administrativo ao CEO (ou reporte direto).

O Comitê de Auditoria deve ter responsabilidade documentada para nomear e destituir o CAE no estatuto de auditoria interna.

Comentários:

As linhas de reporte do CAE devem ser criadas para apoiar a preservação da independência dentro de uma organização e promover a posição da auditoria interna ao lado da equipe de liderança.

O CAE deve ter acesso contínuo e regular ao Presidente do Comitê de Auditoria, com acesso a outros Membros do Comitê de Auditoria, conforme necessário. Seria prudente que uma sessão 'à porta fechada'[3] entre o CAE e o Comitê de Auditoria fosse realizada em cada reunião do Comitê de Auditoria.

Ao nomear o CAE, o Comitê de Auditoria deve equilibrar habilidades e capacidades técnicas com atributos como coragem, inteligência emocional, e gestão e engajamento com os stakeholders.[4]

Referências às Normas do IIA (IPPF):

1100 – Independência e Objetividade

1110 – Independência Organizacional

1111 – Interação Direta com o Conselho

Recomendação 1.3

Os chefes das subsidiárias, filiais e chefes individuais de auditoria interna devem reportar ao CAE do grupo, mantendo o reconhecimento da legislação e regulamentação local.

Comentários:

Os chefes das subsidiárias, filiais e divisões de auditoria interna devem reportar principalmente ao CAE, embora reconhecendo a legislação ou regulamentação local, conforme apropriado. Isso inclui a responsabilidade de definir orçamentos e remuneração, realizar avaliações e revisar o plano de auditoria interna.

O CAE do grupo deve considerar a independência, objetividade e mandato dos chefes de subsidiária, filial ou divisão de auditoria interna ao realizar as avaliações.[5]

Recomendação 1.4

O escopo da auditoria interna deve ser irrestrito e englobar toda a organização. No mínimo, a auditoria interna deve incluir as seguintes áreas em seu escopo:

a. **Governança, estruturas e processos de riscos;**
b. **Cultura de risco e controle da organização;**
c. **Risco de mau tratamento ao cliente; e**
d. **Principais eventos corporativos.**

Comentários:

Em geral, as seguintes informações devem ser consideradas, para informar cada área de escopo:

Governança, estruturas e processos de riscos

- A concepção e eficácia operacional da estrutura e processos de governança interna da organização;
- Os processos e controles específicos que apoiam a tomada de decisões estratégicas e operacionais, e se a informação apresentada ao Conselho e à equipe de liderança representa de forma adequada os benefícios, riscos e pressupostos associados à estratégia necessária e/ou modelo de negócio correspondente; e
- O framework de gerenciamento de riscos (conforme exigido pela Prudential Standard CPS 220 e pela SPS 2206 da APRA[6]), incluindo a avaliação da qualidade do trabalho preparado pelas funções de gestão de primeira e segunda linha.

Cultura de risco e controle da organização

- A maneira pela qual os processos, ações, tom no topo e comportamentos observados em toda a organização estão alinhados com os valores fundamentais da organização, ética, políticas e apetite a risco; e
- A atitude observada e abordagem ao gerenciamento de riscos e controles internos, incluindo as ações da gestão para resolver deficiências de controle conhecidas e a avaliação contínua dos controles.

2 Doravante, tais cargos serão coletivamente referidos como Chefe Executivo de Auditoria (CAE)
3 'À porta fechada' refere-se a uma sessão realizada de forma privada
4 Consulte a Recomendação 2.1 (b)(v)
5 Consulte a Recomendação 2.4
6 De acordo com o parágrafo 45 da CPS 220 Risk Management e o parágrafo 27 da SPS 220 Risk Management

Risco de mau tratamento ao cliente

- Se a organização atua com integridade nas relações com os clientes e em interações mais amplas com o mercado; e
- A maneira pela qual a gestão de negócios e a de riscos estão criando e controlando produtos, serviços e processos de suporte para se alinhar aos interesses dos clientes e regulamentar a conduta.

Principais eventos corporativos

- Mudanças significantes nos processos de negócio, introdução de novos produtos e serviços, terceirização, aquisições ou desinvestimentos; e
- A auditoria interna deve trabalhar em conjunto com o Chief Risk Officer e a função de riscos em tempo real, para avaliar o nível apropriado de envolvimento da auditoria interna em eventos corporativos que apresentem alto risco à organização.

Para cumprir com suas responsabilidades com eficácia, a auditoria interna deve ter acesso tempestivo às principais informações de gestão e direito de acesso aos registros relevantes da organização.

A auditoria interna não deve adotar uma abordagem de 'checklist' com base apenas na concepção de processos e controles, mas deve considerar os resultados que resultarão de sua aplicação, conforme avaliado em relação aos valores essenciais, ética, políticas e apetite a risco da organização.

Referências às Normas do IIA (IPPF):

2110 – Governança

2120 – Gerenciamento de Riscos

2130 – Controle

Recomendação 1.5

O universo de auditoria e o plano de auditoria interna devem ser baseados no risco e independentemente definidos pela auditoria interna, com base em consulta razoável aos stakeholders da organização e sujeitos à revisão, contestação e aprovação do Comitê de Auditoria.

Comentários:

A auditoria interna deve exercer seu próprio julgamento para determinar a segmentação mais eficaz do universo de auditoria, dada a estrutura e o perfil de risco da organização. Pelo menos anualmente, a integridade do universo de auditoria deve ser verificada (isto é, se captura todos os funcionários ou hierarquias financeiras dentro da organização).

Ao estabelecer suas prioridades e decidir onde realizar um trabalho mais detalhado, a auditoria interna deve adotar um plano de auditoria interna baseado em riscos, para se concentrar nas áreas onde considera os riscos mais elevados. O plano não precisa cobrir todas as áreas de escopo a cada ano, mas também não deve ser restrito por falta de recursos, capacidades ou habilidades. Seu julgamento sobre quais áreas devem ser cobertas no plano de auditoria interna e a frequência e método de cobertura do ciclo de auditoria devem estar sujeitos a contestação e aprovação pelo Comitê de Auditoria.

O plano de auditoria interna deve ser criado para ser flexível, para responder a eventos não planejados e permitir que a auditoria interna priorize riscos emergentes, com quaisquer mudanças no plano consideradas à luz da avaliação contínua de riscos da auditoria interna. Esse processo deve incluir a colaboração com os principais stakeholders (incluindo o Comitê de Auditoria e a alta administração), a fim de compreender o ambiente operacional da organização, riscos atuais e emergentes, iniciativas estratégicas e impactos regulatórios. Quaisquer mudanças materiais feitas no plano de auditoria interna devem ser aprovadas pelo Comitê de Auditoria.

Referências às Normas do IIA (IPPF):

2010 – Planejamento

2020 – Comunicação e Aprovação

Garantir recursos e senioridade adequados

A composição, estrutura e acordos de remuneração da auditoria interna devem apoiar uma avaliação independente e eficaz.

Recomendação 2.1

O CAE deve ser membro de um órgão profissional relevante, com um código de conduta profissional apropriado e um processo disciplinar para membros. Os exemplos incluem o Institute of Internal Auditors (IIA) e os Chartered Accountants Australia e New Zealand (CA ANZ). O CAE deve garantir que a equipe de auditoria interna:

a. **Possua capacidade, habilidade, competência e experiência coletivas abastecidas interna e externamente para executar o plano de auditoria interna e influenciar os stakeholders em toda a organização.**

b. **Tenha um equilíbrio entre os membros da equipe proporcional ao tamanho e complexidade da organização, tendo entre eles:**

   i. **Credenciamentos por órgãos profissionais ou certificação profissional como auditor interno;**

   ii. **Experiência empresarial na organização ou organizações pares;**

   iii. **Qualificações ou experiência em disciplinas relacionadas, incluindo, mas não se limitando a finanças, análise de dados, tecnologia da informação e gerenciamento de riscos. Alguns membros da equipe de auditoria interna também podem ter qualificações ou experiência em gestão de projetos, psicologia organizacional, investigações ou liderança;**

   iv. **Capacidades relevantes para influenciar os stakeholders, incluindo, mas não se limitando à capacidade de entregar comunicações verbais e escritas claras e concisas, bem como habilidades em negociação, resolução de conflitos, governança e gestão de mudanças;**

   v. **Além disso, todos os membros da equipe devem possuir atributos pessoais de coragem e resiliência, e aplicar e defender os princípios de integridade, objetividade, confidencialidade e competência (conforme exigido pelo Código de Ética do IIA).**

c. **Implante ou endosse um programa de gestão de talentos, para atrair e reter os principais talentos de auditoria interna.**

Comentários:

A composição da equipe de auditoria interna deve levar em consideração as necessidades de avaliação dos stakeholders da organização e objetivos de negócios, estratégias, riscos associados e processos de gerenciamento de riscos, operações, programas, sistemas e controles. A combinação de conhecimentos, habilidades e competências deve responder dinamicamente às mudanças nos objetivos de negócios, riscos e necessidades de avaliação dos stakeholders.

Para conseguir isso, o CAE deve considerar o uso de recursos da equipe de auditoria interna, capacidades internas (como especialistas técnicos), recursos cedidos ou adquiridos de outras partes da organização e capacidades externas compartilhadas (co-sourcing).

A manutenção da habilidade, capacidade e experiência em uma equipe de auditoria interna deve ser feita por meio de uma combinação de programas de treinamento relevantes, por meio do apoio aos membros da equipe para realizar credenciamentos de pós-graduação ou profissionais, recrutamento contínuo, destacamento de outras partes da organização e co-sourcing com terceiros externos.[7]

Um programa abrangente de gestão de talentos é recomendado para atrair e reter os principais talentos da auditoria interna. Quando recursos internos forem usados, deve haver um plano de desenvolvimento individual para cada membro da equipe, para construir e manter suas habilidades e capacidades de acordo com os riscos da organização e a direção estratégica da equipe de auditoria interna. Cada membro da equipe deve receber treinamento e feedback periodicamente e cumprir com as obrigações de conformidade organizacional.

Quando um recurso de co-sourcing externo for usado, as atividades de auditoria devem estar sujeitas ao mesmo trabalho de avaliação de qualidade que os recursos internos.

Referências às Normas do IIA (IPPF):

1210 – Proficiência

1230 – Desenvolvimento Profissional Contínuo

2030 – Gerenciamento de Recursos

Recomendação 2.2

Convém que a adequação de recursos na equipe de AI para fornecer questionamento eficaz à organização seja revisada pelo Comitê de Auditoria pelo menos uma vez por ano.

Comentários:

Para informar a revisão por parte do Comitê de Auditoria, o CAE deve fornecer ao Comitê de Auditoria uma recomendação sobre a suficiência de recursos com base nas habilidades necessárias para realizar o trabalho (consulte a Recomendação 2.1 acima) e se o orçamento de auditoria interna é suficiente para recrutar e reter funcionários ou adquirir outros recursos com a expertise, experiência e objetividade necessárias para oferecer questionamento eficaz em toda a organização e para a equipe de liderança.

Referências às Normas do IIA (IPPF):

2020 – Comunicação e Aprovação

2030 – Gerenciamento de Recursos

2060 – Reporting to Senior Management and the Board

Recomendação 2.3 [8]

O CAE deve ter um nível de senioridade dentro da organização que permita o acesso apropriado às informações e a autoridade necessária para questionar a equipe de liderança. Os chefes das subsidiárias, filiais e chefes individuais de auditoria interna devem estar em um nível de senioridade comparável aos membros da alta administração cujas atividades eles sejam responsáveis por auditar.

Comentários:

Para facilitar o questionamento devido da equipe de liderança e da alta administração, os membros da equipe de auditoria interna devem ter cargo proporcional aos stakeholders envolvidos nas atividades que estão responsáveis por auditar. A auditoria interna deve ter o direito de comparecer e observar todas ou parte das reuniões da equipe de liderança, e quaisquer outros fóruns de governança e tomada de decisão da gestão.

Referências às Normas do IIA (IPPF):

1000 – Propósito, Autoridade e Responsabilidade

7 Comparável com o parágrafo 21 do *CIIA Guidance on Effective Internal Audit in the Financial Services Sector,* 2ª edição, setembro de 2017 (o Código do Reino Unido)
8 Consulte a Recomendação 1.2

Recomendação 2.4

Quando o mandato do CAE excede um período predeterminado, o Comitê de Auditoria deve realizar uma avaliação anual da independência e objetividade contínuas do CAE.

Comentários:

Com base no apetite da organização, quando a permanência do CAE ultrapassar um prazo predeterminado, o Comitê de Auditoria deve realizar uma avaliação anual da independência e objetividade contínuas do CAE.

O Comitê observa que as práticas atuais de permanência variam entre o setor de serviços financeiros. A maioria das entidades australianas não tem uma política de mandato para o CAE, confiando, em vez disso, nas políticas de independência do auditor. Das entidades que têm políticas de mandato predeterminadas para o CAE, algumas se alinham com os requisitos de rotatividade de profissionais de auditoria externa (cinco anos), algumas usam o *Handbook of the Code of Ethics for Professional Accountants* da *International Federation of Accountants*, que também se alinha com o *UK Code* (sete anos), alguns se referem aos *ASX Corporate Governance Council's Corporate Governance Principles and Recommendations* (dez anos) e outros determinaram suas próprias políticas de mandato para o CAE (p. ex., oito anos).

Cada entidade deve desenvolver sua própria política de mandato para o CAE e, ao atingir esse prazo, anualmente, deve considerar se a exigência de uma mudança de CAE seria pelo melhor interesse da entidade e de seus stakeholders, tendo em conta o provável desempenho futuro, independência e objetividade do CAE titular em relação às opções alternativas de CAE.

Recomendação 2.5

O estatuto de auditoria interna e o estatuto do Comitê de Auditoria devem delinear o processo de avaliação de desempenho para o CAE e devem garantir que o Presidente do Comitê de Auditoria aprove os objetivos de desempenho do CAE, forneça feedback de desempenho e aprove as avaliações de desempenho do CAE.

Comentários:

O processo de avaliação de desempenho do CAE e de qualquer chefe de subsidiária, filial e chefes individuais de auditoria interna deve ser descrito no estatuto de auditoria interna e no estatuto do Comitê de Auditoria.

Para elevar a independência e objetividade do CAE, o Presidente do Comitê de Auditoria deve aprovar os objetivos do CAE, fornecer feedback de desempenho pelo menos anualmente e aprovar a classificação de desempenho do CAE. Os objetivos e o processo de avaliação de desempenho também geralmente levam em consideração os pontos de vista do CEO e de outros gerentes seniores, e devem ser consistentes com as responsabilidades individuais.

Muitos CAEs de organizações de serviços financeiros serão 'responsáveis' sob o *Banking Executive Accountability Regime* (BEAR) ou o *Financial Accountability Regime* (FAR).

Independentemente de se aplicar o BEAR ou o FAR, o CAE, juntamente com qualquer chefe de subsidiária, filial e chefes individuais de auditoria interna, deve ter uma declaração clara de responsabilidade individual, declarando claramente suas responsabilidades. A declaração deve descrever as ações, decisões e resultados pelos quais o indivíduo é responsável e a(s) parte(s) da organização à(às) qual(is) as responsabilidades se relacionam. Essa declaração deve ser aprovada pelo Presidente do Comitê de Auditoria e revisada imediatamente quando houver qualquer alteração no titular ou nas responsabilidades.

A aceitação da responsabilidade individual deve ser indicada na forma de um documento assinado com uma data efetiva. O não cumprimento material com as expectativas delineadas nas declarações de responsabilidade individual e nos objetivos anuais de desempenho deve levar a consequências diretas e proporcionais, que podem incluir redução do salário base ou da remuneração variável, perda de senioridade e, no caso mais extremo, demissão. O Comitê Disciplinar e de Revisão do IIA-Austrália também investiga reclamações e determina ações disciplinares para membros que violarem a Constituição ou o Regulamento Interno do IIA-Austrália ou o Código de Ética do IIA.

Recomendação 2.6

O framework de remuneração do CAE e da equipe de auditoria interna deve ser estruturado de forma a evitar conflitos de interesses, não prejudicar a independência e a objetividade e não estar exclusivamente vinculado ao desempenho de curto prazo da organização.

Comentários:

O framework de remuneração do CAE e da equipe de auditoria interna deve ser desenvolvido para cumprir com as atuais Normas e Diretrizes Prudenciais da APRA.

Compete ao Presidente do Comitê de Auditoria recomendar a remuneração do CAE ao Comitê de Remuneração.

PRINCÍPIO 3

Prestar avaliação que agregue valor

A auditoria interna deve ser eficaz e agregar valor ao atender às necessidades e expectativas de avaliação do Conselho e dos stakeholders.

Recomendação 3.1

O CAE deve fornecer ao Comitê de Auditoria uma declaração anual que ateste a adequação das atividades de auditoria interna e que a estrutura de governança da auditoria interna, plano anual, modelo e reporte da equipe são adequados para a organização, tendo em conta as necessidades de avaliação do Conselho e dos stakeholders, e o tamanho, combinação de negócios e complexidade da organização.

Comentários:

A maioria dos CAEs fornece um atestado anual quanto ao cumprimento com o estatuto de auditoria interna. Muitos CAEs de serviços financeiros também fornecerão um atestado anual quanto ao cumprimento com suas responsabilidades de função no âmbito do BEAR ou FAR.

A partir do momento em que esses atestados não cobrirem o seguinte material, os CAEs devem fornecer uma declaração anual suplementar ou obter uma revisão independente quanto à adequação e pertinência das atividades de auditoria interna. A declaração anual deve confirmar, quanto ao ano anterior encerrado, de acordo com o conhecimento do CAE e tendo feito as investigações adequadas, em todos os aspectos materiais, que:

a. A auditoria interna manteve sua independência e está em conformidade com o Código de Ética, os Princípios Fundamentais, o Framework Internacional de Práticas Profissionais do Institute of Internal Auditors e o Guia de Melhores Práticas de Auditoria Interna para Serviços Financeiros na Austrália;

b. O plano de auditoria interna, capacidade e recursos são apropriados para a organização, levando em consideração as necessidades de avaliação do Conselho e dos stakeholders e o tamanho, a combinação de negócios e a complexidade da organização;

c. As principais descobertas e observações da auditoria interna foram reportadas com precisão à gestão e ao Comitê de Auditoria;

d. As respostas propostas pela gestão às principais descobertas da auditoria interna, estabelecidas como ações de resolução dentro ou após os relatórios de auditoria emitidos durante o ano, foram adequadas no momento da emissão; e

e. Os principais resultados decorrentes de quaisquer observações de auditoria interna relevantes sobre o status das ações de resolução acordadas para descobertas de auditoria levantadas anteriormente foram reportados com precisão à gestão e ao Comitê de Auditoria.

Ao fazer a declaração anual, o CAE deve levar em consideração o nível apropriado de materialidade para a organização e os stakeholders. Questões ou não conformidades imateriais não devem levar diretamente a uma qualificação da declaração. Entretanto, o CAE pode desejar incluir questões relevantes de ênfase para a consideração do Comitê de Auditoria. A divulgação de tais assuntos deve ser feita com o objetivo de auxiliar o Comitê de Auditoria a entender quaisquer limitações específicas da organização sobre a avaliação fornecida pela auditoria interna e, assim, minimizar qualquer lacuna de expectativas.

No caso de o CAE não ser capaz de fornecer uma declaração anual não qualificada, uma justificativa deve ser fornecida ao Comitê de Auditoria, descrevendo as qualificações ou isenções de responsabilidade relevantes e estabelecendo um plano de ação proposto para fechar as lacunas identificadas.

No que diz respeito à declaração sobre a adequação das respostas propostas pela gestão às principais conclusões da auditoria, a intenção é apenas destacar as áreas em que tenha havido desacordo material com a gestão sobre a adequação das ações acordadas no momento da emissão do relatório, ou onde uma ação acordada tenha sido atrasada inaceitavelmente. Essa parte da declaração não se destina a indicar se as ações da gestão foram ou não implantadas.

Referências às Normas do IIA (IPPF):

2060 – Reportando à Alta Administração e ao Conselho

Recomendação 3.2

A auditoria interna deve ser eficaz e agregar valor ao atender às necessidades e expectativas de avaliação do Conselho e de outros stakeholders relevantes.

Comentários:

Uma compreensão das expectativas do Conselho e de outros stakeholders relevantes é fundamental para a capacidade da auditoria interna de entregar valor. A auditoria interna agrega valor à organização e aos stakeholders quando presta avaliação objetiva e relevante e contribui para a eficácia e eficiência dos processos de governança, gerenciamento de riscos e controle. A auditoria interna deve agregar esse valor por meio da eficácia de suas relações com o Conselho, com a gestão e com outros stakeholders, da qualidade e tempestividade de seus relatórios de avaliação e recomendações, e de sua contribuição independente para a avaliação geral dos riscos e para a maturidade de controle da organização.

Os relatórios de avaliação da auditoria interna devem ser direcionados às áreas que agregarão valor ao Conselho e aos stakeholders envolvidos no desenvolvimento do plano de auditoria interna, particularmente o risco.[9]

Referências às Normas do IIA (IPPF):

2000 – Gerenciamento da Atividade de Auditoria Interna

Recomendação 3.3

A independência da auditoria interna como prestador de avaliação e a objetividade de seu trabalho devem ser salvaguardadas.

Comentários:

A independência e a objetividade constituem uma das Normas de Atributos fundamentais do IIA Global[10] e devem ser mantidas nos níveis organizacional e individual.

Enquanto mantém sua independência e objetividade, a auditoria interna deve utilizar seus recursos para ajudar a organização a melhorar a cultura, sistemas, processos e controles de risco.

Consequentemente, em alguns casos, será apropriado que a auditoria interna atue como conselheira confiável, especialista ou investigadora para a organização. No entanto, embora a auditoria interna possa prestar assessoria especializada sobre o desenvolvimento de controles de primeira e segunda linha, a função não deve assumir responsabilidade por seu desenvolvimento, implantação ou operação.

Os auditores internos são destinatários estatutários elegíveis de divulgações de denunciantes.[11] Consequentemente, ser proprietários de uma política ou processo de denúncia, ou conduzir uma investigação de um assunto levantado por um denunciante, é consistente com o papel da auditoria interna como prestador independente de avaliação.

Referências às Normas do IIA (IPPF):

1100 – Independência e Objetividade

Recomendação 3.4

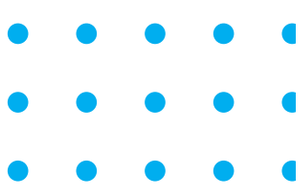
A auditoria interna deve definir uma estratégia que seja aprovada pelo Comitê de Auditoria.

Comentários:

A visão e a estratégia da auditoria interna devem ser aprovadas pelo Comitê de Auditoria e comunicadas ao Conselho e outros stakeholders relevantes. A estratégia deve estabelecer uma metodologia para a realização de auditorias internas, incluindo critérios de qualidade e uma provisão para benchmarking externo regular.

Referências às Normas do IIA (IPPF):

2040 – Políticas e Procedimentos



9 Consulte também a Recomendação 1.5
10 Norma 1100 – Independência e Objetividade – Normas de Atributos do IIA-Global
11 Seção 1317AAC da lei *Treasury Laws Amendment (Enhancing Whistleblower Protections)* de 2017

Recomendação 3.5

Os processos operacionais da AI devem ser estabelecidos e gerenciados de acordo com a estratégia aprovada.

Comentários:

O CAE deve gerenciar a auditoria interna por meio de:

- Desenvolvimento periódico de um plano abrangente de auditoria com base em riscos;
- Garantir que todas as auditorias internas sejam realizadas de acordo com a metodologia e critérios de qualidade estabelecidos;
- Interação regular com os principais stakeholders do negócio, para entender as mudanças do negócio, buscar contribuições para o plano de auditoria interna e assessorar sobre o andamento das auditorias e questões materiais;
- Aprovação da publicação de quaisquer relatórios de trabalho de auditoria, incluindo recomendações de melhoria;
- Definição de principais indicadores de desempenho em relação à auditoria interna;
- Reportar regularmente ao Comitê de Auditoria e outros stakeholders relevantes os resultados de quaisquer auditorias, bem como o desempenho da própria AI;
- Garantir o acompanhamento adequado das questões materiais, incluindo a resolução eficaz das suas causas raízes;
- Implantar o framework de risco e conformidade da organização no que diz respeito às obrigações de risco e conformidade da auditoria interna; e
- Encaminhar questões de preocupação ao CEO ou Presidente do Comitê de Auditoria, quando apropriado.

Referências às Normas do IIA (IPPF):

2340 – Supervisão do Trabalho de Auditoria

Recomendação 3.6

Estabelecer e manter a capacidade de cumprir com a estratégia de auditoria e com o plano anual de auditoria interna.

Comentários:

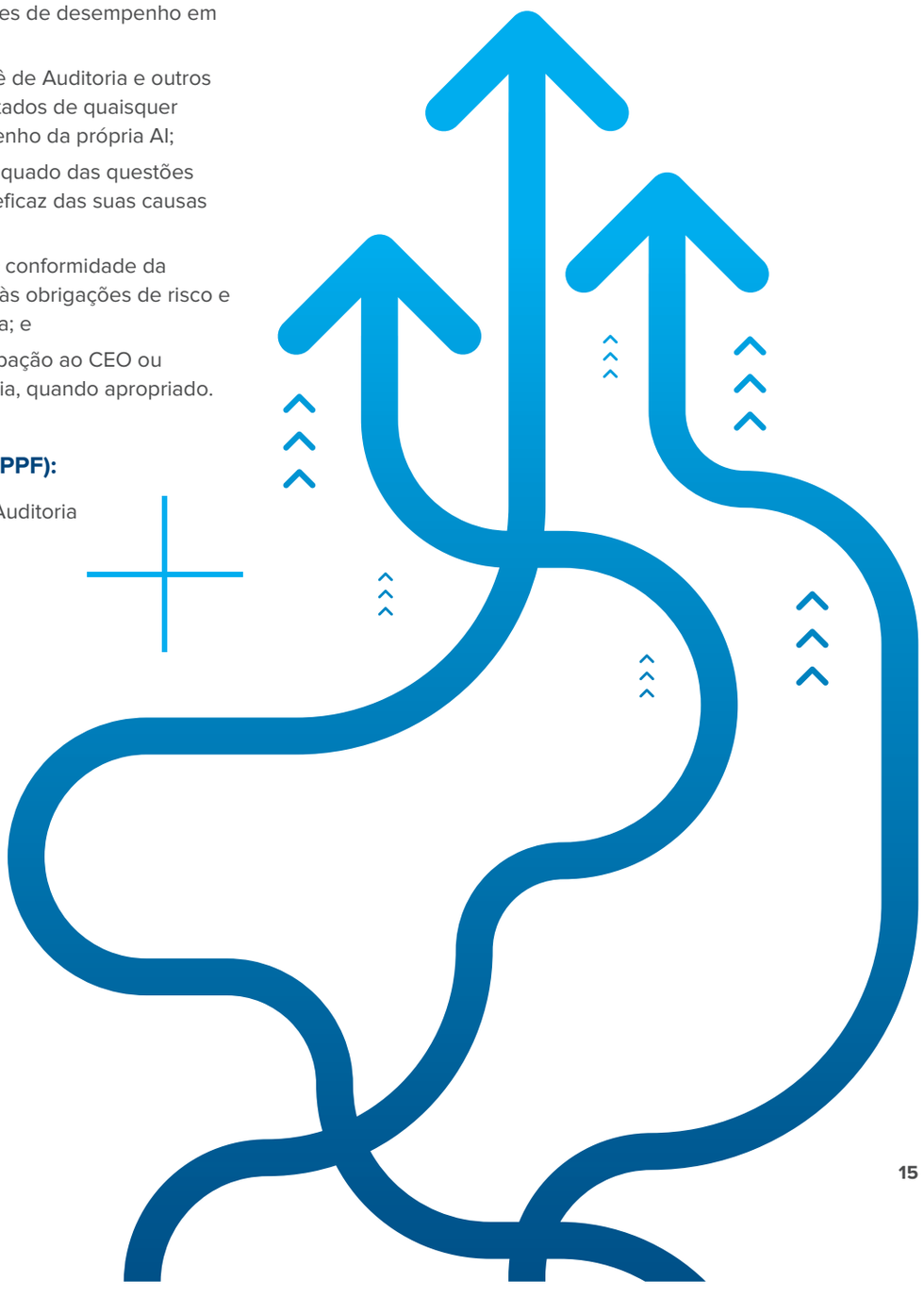
Estabeleça uma equipe de auditoria interna com recursos adequados e a combinação certa de habilidades e competências para executar a estratégia de auditoria e o plano anual. Isso pode incluir o uso de recursos externos compartilhados (co-sourcing).[12]

Referências às Normas do IIA (IPPF):

2030 – Gerenciamento de Recursos

2050 – Coordenação e Confiança

2230 – Alocação de Recursos ao Trabalho de Auditoria



12 Consulte a Recomendação 2.1

Empregar métodos e ferramentas apropriadas à tarefa

A auditoria interna deve manter uma metodologia atualizada, assim como suas práticas subjacentes e ferramentas associadas, para aumentar sua eficácia.

Recomendação 4.1

A auditoria interna deve manter um conjunto atualizado de políticas e procedimentos, e de métricas de desempenho e eficácia.

Comentários:

As políticas e procedimentos devem orientar a atividade de auditoria interna, articular claramente a metodologia de auditoria usada, alinhar-se com as Normas e orientações do IIA, fazer referência ao estatuto ou mandato da função e consultar as técnicas de auditoria descritas neste guia. Além disso, devem abranger os tipos de resultados esperados da auditoria interna, incluindo o tipo de trabalhos de auditoria, níveis de avaliação e opiniões associadas, classificações de significância das questões e reporte da gestão.

Métricas de desempenho e eficácia devem ser implantadas e usadas para avaliar a eficácia da auditoria interna.

Referências às Normas do IIA (IPPF):

2040 – Políticas e Procedimentos

Recomendação 4.2

A AI deve ter um processo estruturado, documentado e baseado em riscos de avaliação contínua de riscos (CRA), conduzido e concluído periodicamente.

Comentários:

O processo de CRA (*continuous risk assessment*) deveria identificar riscos emergentes e variáveis significantes, incluindo os principais fatores internos (p. ex., mudanças de negócios, incidentes e questões) e fatores externos (p. ex., mudanças regulatórias e da indústria), confirmar a avaliação de riscos da AI em todo o negócio e garantir que o plano de auditoria tenha como foco os riscos materiais para a organização.

O produto do processo de CRA deve ser documentado e pode incluir mudanças nas avaliações de riscos do universo de auditoria, mudanças no plano de auditoria, novas questões de auditoria levantadas ou mensagens principais para a equipe de liderança e/ou Comitê de Auditoria. O plano de auditoria também deve ter flexibilidade (p. ex., horas não alocadas) para permitir que a AI priorize o trabalho decorrente da CRA ou de solicitações regulatórias sem impactar negativamente o plano geral de auditoria. Mudanças materiais no plano de auditoria devem ser aprovadas pelo Comitê de Auditoria.

A frequência da CRA será determinada pelo tamanho e natureza da organização.

Referências às Normas do IIA (IPPF):

2010 – Planejamento

2020 – Comunicação e Aprovação

Recomendação 4.3

A auditoria interna deve:

a. **Considerar a aplicação da análise de dados (AD) em todas as fases do ciclo de auditoria;**
b. **Avaliar o risco dos dados;**
c. **Começar pela captura e validação dos dados em tempo hábil, antes de analisar os dados; e**
d. **Implantar treinamento para garantir que sua equipe de auditoria interna tenha recursos suficientes de AD.**

Comentários:

Quando apropriado e compatível com a maturidade de risco da organização, a auditoria interna deve mudar o foco dos procedimentos tradicionais de auditoria com base em amostra para um foco crescente na utilização da análise de dados (AD), para aumentar a eficácia e eficiência de suas atividades de auditoria.

O uso das técnicas de AD dependerá da qualidade e disponibilidade dos dados, dos sistemas usados para capturar e processar os dados e dos recursos de auditoria interna. Também será dependente da extensão da AD baseada em controles utilizada pelas funções de gestão de primeira e segunda linha.

A AD deve ser usada em todo o ciclo de vida da auditoria e se tornará ainda mais importante conforme as organizações aumentarem sua confiança na automação e no uso de robótica e inteligência artificial.

Durante o planejamento da auditoria, a auditoria interna deve considerar uma avaliação do risco dos dados, juntamente com outros riscos principais, e buscar validar os controles avaliando os dados subjacentes.

Para que a AD seja implantada com sucesso, é necessário um planejamento avançado, para que haja tempo suficiente para capturar e validar os dados antes que sejam analisados. Isso inclui identificar os dados disponíveis, extrair os conjuntos de dados necessários e testar a qualidade dos dados usando as técnicas apropriadas de AD.

A AD também pode ser usada para monitoramento ou teste contínuo.

Avaliações de habilidades e treinamento contínuos devem ser realizadas, para garantir que as habilidades de AD da auditoria interna estejam acompanhando os avanços do setor.

Referências às Normas do IIA (IPPF):

1220 – Zelo Profissional Devido

Recomendação 4.4

A auditoria interna deve ter uma metodologia robusta de análise de causa raiz.

Comentários:

A metodologia de análise de causa raiz deve considerar os controles formais (p. ex., políticas e procedimentos, funções e responsabilidades) e elementos comportamentais (p. ex., clareza, comprometimento, viabilidade e se são incentivados) e (no mínimo) deve ser aplicada a todas as questões levantadas pela auditoria. Isso irá garantir que os planos de ação da gestão abordem a causa raiz dos problemas levantados e, portanto, levem a resultados de remediação mais sustentáveis para a organização.

A análise da causa raiz também deve avaliar se o problema (e a causa raiz) pode ser relevante para outras áreas da organização.

Recomendação 4.5

A auditoria interna deve ter uma revisão retrospectiva/um processo de 'lições aprendidas' em vigor, quando a organização estiver sujeita a incidentes significantes e ações regulatórias.

Comentários:

O principal objetivo das revisões retrospectivas é melhorar a auditoria interna. A revisão retrospectiva deve avaliar a adequação da auditoria interna com referência a incidentes significantes e ações regulatórias (incluindo metodologia e cobertura de auditoria). A auditoria interna também deveria avaliar se a função poderia ter identificado eventos externos significantes com impacto sobre outras instituições.

Além disso, a auditoria interna deveria verificar se a organização realizou um exercício de 'lições aprendidas' (isto é, se avaliou as funções de gestão de primeira e segunda linha, e considerou se quaisquer melhorias no ambiente de controle são necessárias).

Recomendação 4.6

A auditoria interna deve ter um programa de avaliação de qualidade em vigor, para garantir que a função opere de acordo com suas políticas e procedimentos.

Comentários:

A auditoria interna deve desenvolver uma capacidade de avaliação de qualidade, com o trabalho realizado por indivíduos que sejam independentes da entrega da auditoria. Os indivíduos que realizam as avaliações devem ter cargo e experiência para questionar significativamente o desempenho da auditoria interna e para garantir que os julgamentos e as opiniões da auditoria interna sejam devidamente evidenciados.

O escopo da revisão de avaliação de qualidade deve incluir o entendimento da AI e a identificação de riscos e questões de controle, além do cumprimento com a metodologia e os procedimentos de auditoria. Isso pode exigir o uso de recursos de terceiros. O trabalho de avaliação de qualidade deve ser baseado em riscos, para cobrir os riscos mais elevados da organização e do processo de auditoria. Os resultados dessas avaliações devem ser apresentados diretamente ao Comitê de Auditoria pelo menos uma vez ao ano. Quando a AI é terceirizada para um prestador externo, o trabalho da auditoria interna deve estar sujeito ao mesmo trabalho de avaliação de qualidade que as funções internas. Os resultados desse trabalho de avaliação de qualidade devem ser apresentados ao Comitê de Auditoria pelo menos uma vez por ano para revisão.

Referências às Normas do IIA (IPPF):

1300 – Programa de Avaliação e Melhoria da Qualidade

1310 – Requisitos do Programa de Avaliação e Melhoria da Qualidade

1311 – Avaliações Internas

1320 – Divulgações do Programa de Avaliação e Melhoria da Qualidade

Recomendação 4.7

A auditoria interna deve confiar (isto é, 'alegar' cobertura de auditoria) no trabalho de outro prestador de avaliação somente após uma avaliação da eficácia do trabalho do prestador ter sido realizada.

Comentários:

A confiança em outros prestadores de avaliação para 'alegar' cobertura de auditoria pode resultar em trabalhos de auditoria mais eficientes, permitindo que a função aloque seus recursos para outras áreas de cobertura de auditoria. (Obs.: Esta recomendação não é aplicável para o trabalho realizado como parte de uma relação de co-sourcing, onde a função de auditoria interna retém a 'propriedade' do trabalho de auditoria (incluindo escopo e qualidade/revisão dos papéis de trabalho).)

A avaliação da eficácia deve ser realizada pelo menos a cada dois anos e incluir uma avaliação das seguintes áreas:

- Governança: mandato/estatuto, independência e objetividade;
- Propósito: independência e objetividade;
- Recursos: capacidade e habilidade de cumprir com o mandato;
- Competência;
- Políticas e procedimentos (incluindo avaliação de qualidade);
- Elementos de prática;
- Reporte e remediação de questões: reporte ao Comitê; relatórios de avaliação; rastreamento e validação de questões;
- Comunicação de resultados e remediação impactante.

Uma opinião de confiabilidade deve ser emitida para concluir esta avaliação, com questões levantadas conforme apropriado.

Se o prestador de avaliação for avaliado como eficaz e o escopo do trabalho do prestador de avaliação estiver alinhado com parte ou com todo o escopo de auditoria, pode-se confiar no trabalho do prestador de avaliação, se for executado um trabalho de reavaliação para confirmar que a auditoria interna chegaria à mesma conclusão. Essa reavaliação deve envolver uma nova execução da amostra baseada em riscos do trabalho (passo a passo do processo, teste da eficácia do desenvolvimento e operação de controles).

Se forem identificados problemas com o trabalho de avaliação, a auditoria interna não deve confiar no trabalho do prestador de avaliação e deve prosseguir com o teste direto do escopo da auditoria, e levantar qualquer questão(ões) em relação ao prestador de avaliação, conforme apropriado.

O trabalho de reavaliação deve ser documentado no arquivo de auditoria de acordo com a prática padrão.

Referências às Normas do IIA (IPPF):

2050 – Coordenação e Confiança

Recomendação 4.8

A auditoria interna deve ser avaliada quanto à conformidade com o Código de Ética e as Normas por um avaliador independente qualificado, externo à organização, pelo menos uma vez a cada cinco anos.

Comentários:

O Comitê de Auditoria deve obter uma avaliação externa independente e objetiva em intervalos apropriados, dependendo do porte e da natureza da organização. Isso pode assumir a forma de revisões periódicas dos elementos da função em relação às melhores práticas (de pares locais e globais) ou uma única revisão da função geral. Em qualquer caso, a auditoria interna deve, no mínimo, estar sujeita a uma revisão pelo menos a cada cinco anos, conforme estabelecido no Framework Internacional de Práticas Profissionais de auditoria interna. Convém que a conformidade da auditoria interna com essa orientação seja explicitamente incluída nessa avaliação. O Presidente do Comitê de Auditoria deve supervisionar e aprovar o processo de nomeação do avaliador independente.

Referências às Normas do IIA (IPPF):

1312 – Avaliações Externas

PRINCÍPIO 5

Reportar para influenciar mudanças positivas

A AI deve causar mudanças positivas, oferecendo informações tempestivas, precisas e perspicazes para uso como base para a tomada de decisões com foco em riscos.

Recomendação 5.1

A auditoria interna deve fornecer reportes formais ao Comitê de Auditoria, bem como a outros Comitês do Conselho, conforme apropriado (p. ex., Comitê de Risco, Comitê de Tecnologia, Comitê de Remuneração, etc.). Além disso, a auditoria interna deve fornecer reportes formais à equipe de liderança, conforme apropriado.

Comentários:

Convém que o reporte de auditoria interna seja formalmente documentado e endossado pelos órgãos reguladores relevantes.

Referências às Normas do IIA (IPPF):

2060 – Reportando à Alta Administração e ao Conselho
2440 – Disseminação dos Resultados

Recomendação 5.2

A auditoria interna deve considerar os seguintes tipos de reporte:

- **Ao Conselho e Comitê do Conselho (p. ex., Comitê de Auditoria, Comitê de Risco, etc);**
- **À equipe de liderança;**
- **De escalonamento em tempo real (conforme necessário para problemas críticos);**
- **Relatórios padrão de auditoria interna;**
- **Revisões específicas;**
- **Revisões temáticas;**
- **Revisões de projeto;**
- **Avaliações limitadas;**
- **Revisões e investigações especiais;**
- **Relatórios não classificados; e**
- **Avaliações de validação/acompanhamento das ações da gestão.**

Comentários:

A natureza e o conteúdo do reporte dependerão das atribuições e necessidades dos respectivos órgãos de governança. Além disso, deve-se considerar a tempestividade devida do reporte (isto é, levantar questões significantes imediatamente, por meio de um protocolo de escalonamento definido, em vez de esperar até que um relatório seja formalmente concluído).

Referências às Normas do IIA (IPPF):

2060 – Reportando à Alta Administração e ao Conselho
2440 – Disseminação dos Resultados

Recomendação 5.3

Independentemente do fórum e do formato, o reporte formal de auditoria interna deve ter uma estrutura padrão.

Comentários:

De acordo com a maturidade de risco da organização, os relatórios de auditoria interna devem considerar incluir:

- Uma classificação geral em apoio à avaliação holística;
- Uma primeira página que inclua todas as principais informações que o CEO ou chefe de divisão precise saber, p.ex. classificação holística, estatísticas da questão por classificação, um resumo executivo perspicaz que inclua temas e questões significantes que justifiquem a avaliação holística;
- Classificações das questões alinhadas à devida atenção, propriedade e prestação de contas do Conselho e da gestão. Essas classificações devem ser aplicadas de forma consistente;
- Questões 'significantes'/principais detalhadas (destacando especificamente quando as questões são repetidas ou reabertas). Quando questões ou temas significantes/principais forem identificados, o relatório deve ser conclusivo, de modo que a gestão tome medidas tempestivas para efetuar mudanças positivas;
- Um resumo das questões conhecidas geridas de forma eficaz;
- Detalhes de outras questões reportáveis;
- Escopo;
- Histórico;
- Lista de distribuição, destacando o(s) principal(is) responsável(is) do *Banking Executive Accountability Regime* (BEAR);
- Questões levantadas de forma clara e concisa, cobrindo:
  - Avaliação da questão
  - Detalhes da questão (destacando especificamente se as questões são repetidas ou reabertas)
  - Causa raiz
  - Uma declaração de impacto alinhada à classificação
  - Recomendações e/ou ações acordadas com prazos apropriados, confirmando que abordarão o risco subjacente de forma sustentável.
  - Uma resposta da gestão incorporada ou anexa geralmente deve ser incluída.

Quando um problema pode sugerir a ocorrência de violação regulatória, a auditoria interna deve entrar em contato com a parte relevante da organização (p. ex., em geral, o setor de *compliance*) para sua consideração sobre a possibilidade de adicionar o incidente ao "registro de violações". Manter um registro de violações é considerada a melhor prática pelos reguladores de serviços financeiros australianos.

- Relatórios especializados que sejam suficientes para permitir o julgamento adequado;
- Foco nos principais riscos e nas principais falhas de controle – os departamentos de auditoria geralmente perdem o impacto e, às vezes, sua reputação ao levantar questões de tão baixo risco que desviam a gestão dos verdadeiros riscos e preocupações.

Referências às Normas do IIA (IPPF):

2410 – Critérios para as Comunicações
2450 – Opiniões Gerais

Recomendação 5.4

Para contribuir para uma governança organizacional eficaz, são necessários reporte e protocolos apropriados do Comitê de Auditoria do Conselho.

- O reporte ao Comitê de Auditoria do Conselho e as aprovações exigidas do Presidente do Comitê de Auditoria devem, no mínimo, incluir o seguinte:
  - Revisão e aprovação do estatuto do departamento de auditoria
  - Plano de auditoria anual para aprovação
  - Aprovação do orçamento
  - Resultados das principais auditorias e questões
  - Reporte periódico de questões atrasadas e antigas que excedam os prazos pré-estabelecidos com base nas classificações. O executivo relevante deve comparecer e discuti-las, com base nas preferências do Conselho
  - Eficácia da auditoria interna, p. ex. resultados de avaliações de qualidade, KPIs, pesquisas com stakeholders, *post-mortems* de incidentes, etc.
- Quando for possível alterar as datas de remediação de questões, o Presidente do Comitê de Auditoria deve ser consultado para determinar se deseja aprovar todas as alterações às datas de remediação de questões significantes aplicáveis à sua jurisdição. Da mesma forma, o Presidente do Comitê de Auditoria deve ser consultado para determinar se deseja revisar as alterações às datas de remediação de questões significantes externas à sua jurisdição, mas que ainda sejam relevantes à mesma, para que tenham a oportunidade de destacar quaisquer preocupações ao Comitê de Auditoria do grupo relevante.
- O Presidente do Comitê de Auditoria deve ser consultado para determinar se deseja que o executivo relevante participe e discuta os relatórios de auditoria interna (vermelhos/insatisfatórios) pelos quais é responsável.

Recomendação 5.5

Quando apropriado, as auditorias internas realizadas podem resultar em contribuições para o processo de gestão de desempenho organizacional, incluindo a gestão de consequências, com o objetivo de reforçar e recompensar a conduta apropriada e abordar a conduta inadequada.

Comentários:

A identificação e a pronta remediação de questões devem ser encorajadas. Como tal, o uso proporcional do framework de gestão de desempenho organizacional é essencial, com base nas circunstâncias individuais identificadas.

Confirmação da consideração de gestão de desempenho

A auditoria interna deve confirmar que existe um processo justo e eficaz para todo o pessoal referido pela auditoria interna para consideração da gestão de desempenho – tanto positivo quanto negativo. O auditor interno chefe deve ser avisado do impacto/resultados de todas as indicações feitas à gestão de desempenho da auditoria interna.

Exemplos de gestão de desempenho positivo

- Forte identificação proativa de riscos e principais controles apropriados;
- Questões autoidentificadas de gestão em torno dos principais riscos; e
- Conduta exemplar com foco na melhoria contínua e na remediação proativa de questões.

Exemplos de gestão de desempenho negativo

A gestão de desempenho negativo pode surgir de duas maneiras distintas, como segue:

- Exemplos relacionados à auditoria, incluindo:
  - Quando um relatório de classificação insatisfatória ou equivalente é emitido e a gestão não estava ciente das questões significantes levantadas que motivaram a classificação. A causa subjacente será o determinante quanto a se a gestão de desempenho negativo deve ocorrer.
  - Conduta obstrutiva ou indevida da equipe durante a execução da auditoria;
  - Falta de sustentabilidade, isto é, questões materiais repetidas ou reabertas em torno dos principais riscos, sem circunstâncias atenuantes; e
  - Questões atrasadas (em relação a um prazo razoável) sem circunstâncias atenuantes justificáveis, p. ex. a gestão priorizou incorretamente e/ou não alocou recursos apropriados (humanos e financeiros) e/ou não teve supervisão/governança eficaz.
- Assuntos identificados em auditorias, mas não relacionados ao processo de auditoria, p. ex.:
  - Quando a equipe indevida e/ou ações/condutas indevidas da gestão forem detectadas em auditorias (p. ex., venda indevida intencional, precificação inadequada, fraude, lavagem de dinheiro intencional/manipulação de *Know Your Customer*, etc.), reportar à alta administração e ao RH para impacto da gestão de desempenho.

Adotar metodologias apropriadas para auditar a cultura de risco

A responsabilidade por definir a cultura de risco é do Conselho da organização. A gestão organizacional, então, tem a responsabilidade de conduzir essa cultura de risco através da organização, mensurando e reportando sobre a cultura de risco, e determinando ações para resolver quaisquer lacunas. Como uma função independente, a auditoria interna pode prestar avaliação independente sobre os processos de governança em torno da cultura e reporte de riscos, mas também uma visão independente da própria cultura de risco. A auditoria interna presta avaliação em relação à cultura de risco, tanto por meio de auditorias das "operações normais de negócios" e quanto por meio de auditorias mais amplas da cultura de risco.

Recomendação 6.1

Uma vez que a cultura de risco é um componente fundamental do framework de gerenciamento de riscos, em suas auditorias de 'operações normais', seja de uma unidade de negócios, processo ou revisão de um evento de risco, a AI deve considerar a dimensão cultural (de riscos).

a. Dado seu papel independente na organização, a AI oferece uma perspectiva crucial sobre a cultura de risco da organização;

b. Quando a primeira ou a segunda linha estão realizando avaliações da cultura de risco, a auditoria interna deve questionar essas avaliações conforme necessário;

c. A auditoria interna deve usar uma variedade de técnicas para produzir percepções da cultura de risco em suas atividades de auditoria;

d. Essas percepções da cultura de risco devem ser apresentadas em relatórios de auditoria quando relevante, incluindo, para entidades reguladas pela APRA, a revisão anual do framework de gerenciamento de riscos; e

e. Os insights da cultura de risco devem ser reportados à gestão e ao Comitê de Auditoria regularmente.

Comentários:

A cultura de risco, um aspecto da cultura organizacional geral, refere-se às normas de comportamento em uma organização relacionadas ao gerenciamento de riscos. Ela é um elemento crucial no framework de gerenciamento de riscos. O Conselho deve garantir a formação de uma visão da cultura de risco na instituição, e até que ponto essa cultura apoia a capacidade da instituição de operar consistentemente dentro de seu apetite a risco, identificar quaisquer mudanças desejáveis para a cultura de risco e garantir que a instituição tome medidas para lidar com essas mudanças. (CPS220, parágrafo 9 (b)). (Entidades de previdência devem consultar SPS220, parágrafo 22 (f)).

Uma cultura de risco favorável significa que os funcionários vão além da 'mera' conformidade com as políticas de risco, comprometendo-se com elas: há uma discussão aberta e regular sobre riscos; preocupações sobre práticas de negócios são levantadas e postas em prática prontamente; e o gerenciamento de riscos é visto como um facilitador do sucesso organizacional. Uma cultura de risco desfavorável pode comprometer a eficácia do framework de gerenciamento de riscos, porque a conformidade com as políticas não é vista como uma prioridade genuína para a organização; outras atividades, como a geração de lucros de curto prazo, podem substituir as considerações de gerenciamento de riscos.

Como a cultura de risco é um componente fundamental do framework de gerenciamento de riscos, os departamentos de auditoria interna devem aspirar a considerar a cultura de risco em auditorias, seja de uma unidade de negócios, processo ou revisão de um evento de risco. Ou seja, a auditoria interna irá, naturalmente, considerar os fatores comportamentais subjacentes que podem estar produzindo os resultados observados. Alternativamente, quando isso não for possível devido a restrições de recursos, uma abordagem baseada em riscos pode ser usada, para determinar quais auditorias incluirão consideração da cultura de risco.

6.1.a Dado seu papel independente na organização, a auditoria interna fornece uma perspectiva crucial sobre a cultura de risco da organização.

O Conselho tem a responsabilidade de formar uma visão da cultura de risco em uma instituição financeira (CPS220, parágrafo 9(b) e CPG220, parágrafo 21). A cultura de risco, referindo-se às normas comportamentais percebidas, é inerentemente difícil de avaliar e pode variar em uma organização. Os diretores, especialmente os não executivos, podem ter dificuldade em formar uma imagem precisa das normas de comportamento da organização.

A auditoria interna está em uma posição ideal para observar as práticas comerciais diárias e as comunicações informais que esclarecem sobre a cultura de risco real, em oposição à desejada. A auditoria interna também está em uma posição ideal para investigar problemas de riscos e violações de políticas, descobrindo os motivadores comportamentais subjacentes que podem apontar para problemas na cultura de risco. Assim, a auditoria interna é uma fonte vital de inteligência para o Conselho no que diz respeito à cultura de risco.

6.1.b A auditoria interna deve questionar as avaliações da cultura de risco das funções de gestão da primeira e segunda linhas, conforme necessário.

Em algumas instituições financeiras, a gestão de primeira e segunda linhas conduz suas próprias avaliações da cultura de risco. Devido à dificuldade de avaliar a cultura de risco conforme já observado, é importante que a auditoria interna forneça sua própria perspectiva. A auditoria interna deve reportar quaisquer inconsistências identificadas entre as diversas avaliações, questionando tanto a metodologia quanto as conclusões, conforme necessário.

6.1.c A auditoria interna deve usar uma variedade de técnicas para auditar a cultura de risco.

A AI deve usar uma variedade de técnicas para avaliar a cultura de risco. Para atingir esse objetivo, pode ser necessário ampliar a expertise da equipe de auditoria interna, conforme observado no Princípio 2. Insights úteis da cultura de risco podem ser obtidos a partir de uma série de técnicas, incluindo:

- Entrevistas e grupos focais;
- Observação de comportamentos, inclusive em reuniões;
- Pesquisas anônimas com a equipe, para quantificar as percepções da cultura de risco na prática;
- Análise de dados relacionados aos resultados do cliente (p. ex., número/natureza das reclamações, tempo necessário para resolver reclamações, rotatividade de clientes, etc.);
- Análise de dados relacionados a análises de desempenho, recompensa e gestão de consequências (p. ex., variação nas classificações de gerentes, adequação de consequências onde foi identificada má conduta, etc.);
- Análise de dados relacionados à eficácia do gerenciamento de riscos (p. ex., violações de apetite a risco, falhas de controle, eventos e violações regulatórias, e tempestividade da remediação de questões)
- Análise de dados da equipe (p. ex., entrevistas de desligamento, sites de classificação de funcionários, rotatividade de pessoal, uso de canais de denúncias confidenciais, etc.);
- Análise do reporte de riscos/questões e as razões para o subreporte e questões repetidas/recorrentes;
- Análise de causa raiz de grandes eventos de risco;
- Análise de dados (p. ex., e-mails, redes sociais, análise textual de reclamações, etc.);
- Comparação de documentos principais (p. ex., planos de negócios, agendas de reuniões, declarações de missão, documentos de política), para verificar o grau de interconectividade e consistência com que abordam a cultura de risco; e
- Avaliação de como as pessoas se comportam durante uma auditoria (se prestam contas, são transparentes, negam, desviam ou desacreditam, etc.).

Quanto à metodologia, a AI deve ser cautelosa com metodologias de pesquisa que não possuem base científica. As práticas problemáticas que podem levar a resultados inválidos incluem:

- Uso de itens de pesquisa que não passaram por um processo de validação rigoroso, principalmente quando desenvolvidos internamente;
- Uso de pesquisas curtas demais para capturar de forma confiável todas as dimensões necessárias da cultura de risco;
- Incluir perguntas sobre a cultura de risco na pesquisa de envolvimento dos funcionários, especialmente quando o envolvimento é um KPI da gestão;
- Pesquisas com convite (todos recebem um link exclusivo), de modo que os funcionários não se sentem seguros para dar respostas honestas; e
- Reporte de resultados a pequenas equipes, de modo que, mais uma vez, os funcionários não se sentem seguros para dar respostas honestas.

6.1.d As percepções da cultura de risco devem ser apresentadas nos relatórios de auditoria interna conforme relevante, incluindo, para entidades reguladas pela APRA, a revisão anual do framework de gerenciamento de riscos.

6.1.e As percepções da cultura de risco devem ser reportadas à gestão e ao Comitê de Auditoria regularmente.

Cada relatório de auditoria, seja de um negócio, processo ou revisão de um evento de risco, é uma oportunidade para a AI fornecer percepções vitais da cultura de risco. Uma discussão da cultura de risco deve ser incluída nos relatórios, sempre que for relevante, porque a cultura de risco provavelmente varia na organização e os eventos de risco geralmente têm um elemento cultural subjacente (risco).

De acordo com o CPS220, parágrafo 44, uma instituição financeira regulamentada pela APRA deve conduzir uma revisão anual da eficácia de seu framework de gerenciamento de riscos. Dada a importância da cultura de risco, a AI deve incluir, na revisão anual, uma visão geral de suas descobertas sobre a cultura de risco.

Independentemente do status regulatório, a auditoria interna deve reportar os insights da cultura de risco à gestão e ao Comitê de Auditoria regularmente.

Recomendação 6.2

A auditoria interna deve conduzir auditorias do framework da cultura de risco em uma base cíclica consistente com o apetite a risco da organização, ou antes, se as circunstâncias mudarem substancialmente ou se uma autoavaliação for solicitada pelo regulador. Uma auditoria do framework da cultura de risco envolveria avaliar:

a. **O framework e o processo para definir a cultura de risco desejada pelo Conselho e a forma como foi comunicada em toda a organização;**
b. **As políticas e procedimentos em vigor (especialmente os que abordam riscos, pessoas e conduta), para garantir que estejam alinhados e apoiem uma cultura de risco favorável;**
c. **O processo pelo qual a organização monitora e reporta sua cultura de risco real e quais ações são tomadas quando a cultura de risco real não é consistente com a cultura de risco desejada; e**
d. **A cultura de risco real da organização, como um todo ou em parte, incluindo observações de auditorias anteriores das 'operações normais'.**

Comentários:

Uma auditoria da cultura de risco deve ser conduzida periodicamente conforme determinado pelo apetite a risco e/ou requisitos regulatórios. Uma auditoria não programada da cultura de risco seria indicada se uma autoavaliação for solicitada pelo regulador ou se houver uma mudança significante nas circunstâncias, como uma mudança na liderança/estratégia. Essa auditoria direcionada da cultura de risco também pode ser provocada por resultados de negócios adversos sérios e inesperados, ou se o Presidente do Comitê de Auditoria, o Presidente do Comitê de Risco ou o CAE julgar por qualquer motivo que tal auditoria é necessária. Uma auditoria do framework da cultura de risco envolveria revisar:

- O processo para definir a cultura de risco desejada pelo Conselho e a forma como foi comunicada em toda a organização (p. ex., houve divulgação adequada ou apenas um e-mail? Há um esforço para fazer a equipe entender o que isso significa ou é apenas assumido que todos sabem o que se espera deles?). A cultura de risco desejada é consistente com a estratégia de negócios? As declarações formais da cultura de risco/valores capturam devidamente as dimensões de risco (ou seja, resiliência a longo prazo) e os resultados dos clientes?
- As políticas e procedimentos em vigor em uma organização, para garantir que estejam alinhados e apoiem a cultura de risco desejada definida pelo Conselho (p. ex., código de conduta, programas de treinamento da equipe, adequação de capital, mensuração do desempenho ajustado ao risco, reporte e análises de risco, conformidade e sistemas de reporte regulatório, remuneração, decisões de negócios, delegações de autoridade, recrutamento, gestão de desempenho, etc.). A prioridade devida é dada a riscos não financeiros (operacional, conformidade, conduta)? As funções de risco/conformidade possuem recursos adequados? Planos de ação da gestão são implantados para atingir a cultura de risco desejada, incluindo o monitoramento e avaliação de sua eficácia?
- O processo pelo qual o negócio (funções de gestão de primeira e segunda linhas) mensura, monitora e reporta a cultura de risco (como já observado, garantindo que haja uma metodologia robusta em vigor, etc.), bem como a forma como ela é reportada ao Conselho e quais ações são tomadas quando os resultados mostram que a cultura não está onde deveria estar.
- A cultura de risco real na organização ou na unidade de negócios: consulte a discussão em 6.1.c com relação às diversas técnicas para auditar a cultura de risco.

Anexos

Anexo A
Modelos operacionais de AI

Há vários modelos operacionais que são utilizados em organizações na Austrália para implantar a auditoria interna. As recomendações neste Guia de Melhores Práticas foram desenvolvidas para serem aplicadas amplamente em todos os modelos operacionais de auditoria interna.

Auditoria Interna In-House (Interna)	O modelo interno é abastecido exclusiva ou predominantemente por funcionários internos e gerenciado internamente por um funcionário da organização. O Chefe Executivo de Auditoria (CAE) ou equivalente será responsável perante o Comitê de Auditoria pela execução das atividades de auditoria interna.
Auditoria Interna Compartilhada (Co-Sourcing)	O modelo de auditoria interna compartilhado é frequentemente conduzido por uma combinação de equipe interna e prestadores de serviços, e gerenciado internamente por um funcionário da organização, geralmente o CAE. É reconhecido que o modelo de co-sourcing opera em um continuum e pode mudar entre as organizações. Isso pode variar desde a contratação de especialistas para fornecer ou informar auditorias internas específicas, o compartilhamento ou colaboração de recursos em auditorias internas com prestadores de serviços, ou a terceirização total de auditorias internas individuais dentro do plano de auditoria interna.
Auditoria Interna Terceirizada	No modelo de auditoria interna terceirizada, os serviços de auditoria interna são prestados por um único prestador de serviços ou por um painel de prestadores de serviços contratados pela organização, sem presença de função interna. O prestador de serviços é gerenciado ativamente por um funcionário com conhecimento e experiência em auditoria interna, frequentemente referido como o patrocinador da auditoria interna, enquanto o prestador terceirizado responde diretamente ao Comitê de Auditoria pelas atividades de auditoria interna.

Anexo B
O Modelo das Três Linhas

O Modelo das Três Linhas, conforme delineado pela declaração de posicionamento *IIA's Three Lines Model* (de 20 de julho de 2020), é um guia para ajudar as organizações a identificar estruturas e processos que melhor auxiliem no atingimento dos objetivos e que facilitem a governança e gerenciamento de riscos fortes. O modelo baseado em princípios reconhece que as organizações diferem consideravelmente em sua distribuição de responsabilidades e não tem a intenção de impor uma estrutura, mas sim de fornecer orientação sobre funções e responsabilidades dentro do modelo, para apoiar o gerenciamento de riscos e governança eficazes. A auditoria interna é uma função de terceira linha, que garante avaliação e assessoria independentes e objetivas sobre todos os assuntos relacionados ao atingimento dos objetivos.

Funções de Primeira Linha *(Gestão)*	› Lideram e direcionam ações (incluindo gerenciamento de riscos) e aplicam recursos para atingir os objetivos da organização. › Mantêm um diálogo contínuo com o órgão de governança e reportam os resultados planejados, reais e esperados vinculados aos objetivos da organização; e risco. › Estabelecem e mantêm estruturas e processos adequados para o gerenciamento de operações e riscos (incluindo controles internos). › Garantem o cumprimento das expectativas legais, regulatórias e éticas.
Funções de Segunda Linha *(Gerenciamento de Riscos e Conformidade)*	› Fornecem conhecimentos complementares, suporte, monitoramento e desafios relacionados ao gerenciamento de riscos, incluindo: › O desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controles internos) no nível de processo, sistemas e entidade. › O atingimento de objetivos de gerenciamento de riscos, como conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação de qualidade. › A disponibilização de análises e relatórios sobre a adequação e eficácia do gerenciamento de riscos (incluindo o controle interno).
Funções de Terceira Linha *(Auditoria Interna e Avaliação Objetiva)*	› Mantêm a responsabilidade principal perante o órgão de governança e independência em relação às responsabilidades da gestão. › Comunicam avaliação e assessoria independentes e objetivas à gestão e ao órgão de governança sobre a adequação e eficácia da governança e do gerenciamento de riscos (incluindo controle interno), para apoiar o atingimento dos objetivos organizacionais e para promover e facilitar a melhoria contínua. › Reportam ao órgão de governança os prejuízos à independência e à objetividade e implantam salvaguardas conforme necessário.

Anexo C
Glossário de termos

Agregar valor	A auditoria interna agrega valor à organização e aos stakeholders quando presta avaliação objetiva e relevante e contribui para a eficácia e eficiência dos processos de governança, gerenciamento de riscos e controle.
Ambiente de controle	A atitude e as ações da equipe de liderança quanto à importância do controle dentro da organização. Isso fornece a disciplina e estrutura para o atingimento dos objetivos primários do sistema de controle interno.
Apetite a risco	O nível de risco que uma organização está disposta a aceitar.
Auditoria interna	Um departamento, divisão, equipe de consultores ou outros profissionais que prestam avaliação objetiva e independente e serviços de assessoria desenvolvidos para agregar valor e melhorar as operações da organização. A auditoria interna ajuda uma organização a cumprir com seus objetivos, aplicando uma abordagem sistemática e disciplinada a avaliar e melhorar a eficácia dos processos de governança, gerenciamento de riscos e controle.
Chefe Executivo de Auditoria	Também conhecido como Chefe de Auditoria Interna, o Chefe Executivo de Auditoria (CAE) descreve a função de uma pessoa em cargo sênior, responsável por gerenciar com eficácia a auditoria interna de acordo com o estatuto de auditoria interna e os elementos obrigatórios do IPPF. Qualquer referência ao CAE deve ser considerada para incluir o 'equivalente a CAE' em uma função de auditoria interna terceirizada.
Código de Ética	O Código de Ética do The IIA estabelece princípios relevantes para a profissão e prática de auditoria interna, e regras de conduta que descrevem o comportamento esperado dos auditores internos.
Comitê de Auditoria	Um subcomitê ao qual o Conselho delegou certas funções. O Comitê de Auditoria é responsável pela supervisão da conformidade da auditoria interna com o Código de Ética, as Normas do IIA e o padrão de auditoria.
Conflito de interesses	Qualquer relacionamento que, na realidade ou na aparência, não seja pelo melhor interesse da organização. Um conflito de interesses prejudicaria a capacidade de um indivíduo de desempenhar suas funções e responsabilidades de forma objetiva.
Conformidade	Cumprimento com políticas, planos, procedimentos, leis, regulamentos, contratos ou outros requisitos.
Co-sourcing externo	Envolver/empregar profissional de uma empresa externa à organização, que tenha conhecimento, habilidade e experiência especiais em uma disciplina específica.
Cultura de risco	A cultura de risco, um aspecto da cultura geral, refere-se às normas de comportamento dentro de uma organização, relacionadas ao gerenciamento de riscos. Essas normas, vinculadas a valores e premissas subjacentes, determinam a capacidade coletiva de identificar, compreender, discutir abertamente e agir sobre o risco atual e futuro da organização.

Equipe de liderança	Também conhecida como C-Suíte, alta administração ou gerência executiva, a equipe de liderança refere-se à equipe de alta administração dentro da organização e é supervisionada pelo Conselho de Administração.
Estatuto de auditoria interna	Um documento formal que define os objetivos, autoridade e responsabilidade da auditoria interna. Estabelece o posicionamento da auditoria interna dentro da organização; autoriza o acesso a registros, pessoal e propriedades físicas relevantes para o desempenho dos trabalhos; e define o escopo das atividades de auditoria interna.
Framework Internacional de Práticas Profissionais	O framework conceitual que organiza as orientações oficiais promulgadas pelo The IIA. As orientações oficiais são compostas por duas categorias: (1) mandatórias e (2) recomendadas.
Gerenciamento de riscos	Um processo para identificar, avaliar, gerenciar e controlar eventos ou situações potenciais para oferecer garantia razoável do atingimento dos objetivos da organização.
Governança	A combinação de processos e estruturas implantados pelo Conselho para informar, dirigir, gerenciar e monitorar as atividades da organização para o cumprimento de seus objetivos.
Independência	A isenção de condições que ameacem a capacidade da auditoria interna de cumprir com as responsabilidades da auditoria interna de forma imparcial.
Norma	Um pronunciamento profissional promulgado pelo *International Internal Audit Standards Board*, que delineia os requisitos para a realização de uma ampla gama de atividades de auditoria interna e para a avaliação do desempenho da auditoria interna.
Objetividade	Uma atitude mental imparcial que permite aos auditores internos realizar trabalhos de forma que acreditem no produto de seu trabalho e sem comprometer a qualidade.
Políticas e procedimentos	As políticas e procedimentos orientam a auditoria interna. A forma e o conteúdo das políticas e procedimentos dependerão do tamanho e da natureza da auditoria interna.
Princípios Fundamentais	Os Princípios Fundamentais para a Prática Profissional de Auditoria Interna são a base para o IPPF e apoiam a eficácia da auditoria interna.
Risco	A possibilidade de ocorrer um evento que tenha impacto sobre o cumprimento dos objetivos. O risco é mensurado em termos de impacto e probabilidade.
Serviço de avaliação	Um exame objetivo das evidências, com o objetivo de prestar avaliação independente sobre os processos de governança, gerenciamento de riscos e controle da organização.
Tom no topo	No contexto da governança de risco, o tom no topo refere-se à cultura de risco que existe no Conselho e entre os executivos seniores. O tom no topo pode ser significante para determinar a cultura de risco em toda a organização. Declarações formais de valores e políticas podem indicar o tom no topo, mas ele também é demonstrado pelo comportamento dos diretores e executivos em relação ao gerenciamento de riscos, por ex. ao assumir o apetite a risco, questionar as práticas de negócios, alocar recompensas e consequências, apoiar as funções de segunda e terceira linha.
Trabalho de auditoria	Uma atribuição específica de auditoria interna, tarefa ou atividade de revisão, como auditoria interna, revisão de autoavaliação de controle, exame de fraude ou consultoria.
Universo de auditoria	Uma lista de todas as entidades auditáveis em uma organização. Uma entidade auditável poderia ser um local, departamento, função, área de demonstrações financeiras, requisito de conformidade ou uma infinidade de outras entidades.

Comitê de Serviços Financeiros do The IIA

O Comitê foi convocado em agosto de 2019. Ele reúne várias empresas, profissionais de auditoria interna, membros do Comitê de Auditoria e reguladores, cada um oferecendo percepções e conhecimentos valiosos sobre questões e práticas de auditoria interna. Seu trabalho principal foi o desenvolvimento deste Guia de Melhores Práticas.

Membros do Comitê

Sandra Birkensleigh (Presidente)
Diretora Não Executiva e Presidente do *Financial Services Committee*

Sue Carter
Diretora Não Executiva, First State Super

Deborah Chesney
Chief Audit Executive, Allianz Austrália

Nicola Rimmer-Hollyman
Chief Audit Executive, AMP

Scott Kieran
Gerente Geral, *Chief Audit Executive, Group Audit,* Westpac Group

Richard Knox
Chefe de Práticas Profissionais, Macquarie Group

John F Minz
Diretor Não Executivo e Presidente de Comitês de Auditoria, RACQ Group

Amanda Morgan
Chief Audit Officer, Rabobank Austrália & Nova Zelândia

Professora Elizabeth Sheedy
Macquarie Business School

Jon Tyers
Gerente Geral de Auditoria, MLC Life Insurance

Muir Watson
Gerente Geral Executivo, Auditoria Interna, IAG

Observadores

Brian Burgess
Especialista em Risco Operacional, Resiliência Operacional, APRA

Kim Demarte
Supervisor Chefe, Governança, ASIC

Peter Jones
Chief Executive Officer, IIA-Austrália

Doug Niven
Contador Chefe, ASIC

Elizabeth Parsons
Chefe de Risco Operacional, Resiliência Operacional, APRA

Tony Rasman
Gerente de Assuntos Públicos, IIA-Austrália

Rob Sharma
Chefe de Contabilidade, Assessoria & Aprovações, APRA

Agradecimentos

O IIA-Austrália agradece as contribuições para esta publicação generosamente fornecidas por:

Hanny Hassan
Sócio, EY

Cindy Martin
Diretora Associada, KPMG

Damien O'Meara
Sócio, EY

Pushpinder Singh
Sócio, KPMG

Alex Timpers
Diretor, EY

O IIA-Austrália também reconhece o uso de material contido no documento *Effective Internal Audit in the Financial Services Sector – Recommendations from the Committee on Internal Audit Guidance for Financial Services,* do *Chartered Institute of Internal Auditors* (UK) (julho de 2013 e 2017).

Mais informações sobre o Comitê está disponível no IIA-Austrália.

Sobre o Institute of Internal Auditors

O *Institute of Internal Auditors* (The IIA) é a associação profissional global para auditores internos, com sede global nos EUA e institutos afiliados em todo o mundo, incluindo na Austrália (IIA-Austrália).

Como principal defensor da profissão de auditoria interna, o IIA atua como o criador de normas internacionais da profissão, o único fornecedor de certificações de auditoria interna aceitas globalmente e o principal pesquisador e educador.

O The IIA define o padrão para a integridade e profissionalismo da auditoria interna em todo o mundo com seu Framework Internacional de Práticas Profissionais (IPPF), uma coleção de orientações que inclui as Normas Internacionais para a Prática Profissional de Auditoria Interna e o Código de Ética.

Copyright

Este guia contém uma variedade de materiais protegidos por direitos autorais. Parte é propriedade intelectual do autor, enquanto parte é propriedade do *Institute of Internal Auditors* (The IIA) ou do *Institute of Internal Auditors* – Austrália. Parte do material é propriedade de terceiros, o que é mostrado por meio de atribuição e referência. Parte do material é de domínio público. Exceto para o material que é inequívoca e indiscutivelmente de domínio público, apenas o material de propriedade do The IIA e do *Institute of Internal Auditors* – Austrália, assim indicado, pode ser copiado, desde que o conteúdo textual e gráfico não seja alterado e a fonte seja reconhecida. O *Institute of Internal Auditors* – Austrália reserva-se o direito de revogar essa permissão a qualquer momento. A permissão não é dada para qualquer uso comercial ou venda do material.

Isenção de Responsabilidade

Embora o *Institute of Internal Auditors* – Austrália tenha tentado garantir que as informações nesta publicação sejam tão precisas quanto possível, as informações são apenas para uso pessoal e educacional e são fornecidas de boa fé, sem qualquer garantia expressa ou implícita. Não há garantia dada à exatidão ou atualidade das informações contidas nesta publicação. O *Institute of Internal Auditors* – Austrália não se responsabiliza por quaisquer perdas ou danos ocasionados pelo uso das informações contidas neste Guia de Melhores Práticas.

Novembro de 2020

T +61 2 9267 9155
E enquiry@iia.org.au

www.iia.org.au