Deloitte.

Auditoria Interna

Riscos e oportunidades para 2022

Índice

Introdução: sobre riscos, oportunidades e auditoria interna

Riscos

O risco é muitas vezes considerado como algo inerentemente negativo, mas uma visão mais detalhada revela uma dualidade complexa. Paralelos podem ser encontrados na literatura — como Dr. Jekyll e Mr. Hyde em "O Médico e o Monstro", risco e oportunidade habitam o mesmo corpo – e na ciência – como a Terceira Lei de Newton, para cada risco há uma oportunidade igual. Não há dúvidas de por que o aspecto negativo do risco predomina. Nos últimos anos, o mundo testemunhou uma confluência sem precedentes de múltiplas ameaças, muitas das quais geraram, entrelaçaram e/ou exacerbaram as outras. Uma lista severamente truncada inclui a pandemia de Covid-19, mudanças climáticas, escassez de mão-de-obra, interrupções da cadeia de suprimentos, ameaças cibernéticas, conflitos e convulsão política e social. Consideradas juntas, essas e outras ameaças abalaram as próprias bases sobre as quais a sociedade e os negócios são construídos.

Oportunidades

No entanto, oportunidade e risco caminham juntos. Considere, por exemplo, o segmento de ESG — que aborda tópicos ligados aos temas ambientais, sociais e de governança. As organizações enfrentam fortes pressões regulatórias e sociais para respeitar os altos padrões, e o fracasso pode levar a danos financeiros, regulatórios e reputacionais significativos. No entanto, se as empresas acertarem em endereçar essas exigências, elas podem fazer grandes coisas, tanto em termos de contribuições positivas para as principais questões globais, quanto na criação de uma vantagem competitiva no mercado.

Auditoria Interna

A auditoria interna, como o próprio risco, muitas vezes é mal compreendida. A profissão sofre historicamente de percepções desfavoráveis, sendo vista como uma função de fiscalização ou como um vigilante que aparece para relatar o que deu errado. No entanto, uma definição mais avançada e moderna de auditoria interna também contém uma dualidade: provedores essenciais de serviços de asseguração e assessoria. A auditoria interna é legitimamente cautelosa com os riscos, e a função sempre será encarregada de proteger suas organizações por meio de asseguração. Entretanto, os times de auditoria interna verdadeiramente evoluídos também buscarão ajudar a gestão a navegar desafios futuros e tomar decisões mais assertivas, aproveitando ao máximo as oportunidades simultâneas que todo risco oferece.

Nesta publicação, apresentamos uma coleção de riscos e oportunidades importantes que as organizações devem ter em seu radar — além da auditoria interna em seus planos de auditoria.

A lista não é exaustiva; nem todos os tópicos se aplicarão a todas as organizações. Cabe a cada entidade avaliar, classificar e priorizar esses riscos e oportunidades em relação ao seu próprio perfil de negócios e circunstâncias. Esse conceito de classificação para focar riscos prioritários é abordado com mais detalhes em nossa publicação "Auditoria Interna 3.0: O futuro da auditoria interna é agora".

Embora o ambiente atual certamente tenha desencadeado muitos sentimentos de incerteza, esse estudo pode servir como contrapeso: uma influência motivadora e destinada à reflexão; um incentivo para colocar sua casa em ordem, suas prioridades em linha reta, e seu plano de ação bem endereçado. Os riscos são abundantes, mas as oportunidades são ainda maiores. E neste cenário a auditoria interna pode fazer a diferença. Funções de auditoria interna que adotam riscos/oportunidades e asseguram/aconselham sobre tais ambiguidades ajudarão suas organizações a saírem mais fortes desses tempos sem precedentes.

O papel da auditoria interna

Gestão de riscos de terceiros

Não combata incêndios. Instale portas à prova de fogo.

Nossa visão

Quando todos os negócios eram vistos de forma isolada, como uma ilha, a auditoria interna era fácil: a maioria dos aspectos da empresa eram tratados internamente, e as preocupações dos auditores internos terminavam na porta da frente da organização.

Hoje, a porta da frente não apenas foi aberta, mas foi derrubada, com as empresas terceirizando parte relevante de suas operações. Enquanto isso, esses terceiros – fornecedores, distribuidores, parceiros e afins – também mantêm suas próprias redes de relacionamentos (sim, até mesmo terceiros têm terceiros) criando um ecossistema massivo de interações que requer, no mínimo, plena consciência e, muitas vezes, até uma supervisão ativa.

A asseguração na gestão de riscos de terceiros em toda empresa exige alguns dados básicos. Comece pedindo à gerência um inventário de todas as relações com terceiros (alerta de spoiler: provavelmente não há uma relação como essa). Quão rapidamente um relatório sobre todo o cenário de relacionamentos e riscos associados aos terceiros pode ser produzido?

Dica: se a resposta for seis meses, eis um problema real. Quantas falhas de terceiros a organização experimentou no último ano? (Resposta esperada: mais do que você pensa.)

Cada relacionamento com terceiros (e demais camadas) carrega seu próprio conjunto de riscos e, para a maioria das organizações, investir em tecnologia será fundamental para mitigá-los. A auditoria interna deve ser preparada para aconselhar a administração e o comitê de auditoria sobre as tecnologias adequadas para monitorar riscos de terceiros, como ferramentas de alerta e análise de tendências em tempo real.

Além disso, é preciso fornecer orientações às partes interessadas sobre as vantagens de obter apoio externo para gestão de riscos de terceiros. Desenvolver recursos internamente pode ser caro e menos ineficiente, já que esse é um nicho que requer especialização e ferramentas adequadas. As mesmas motivações que levam uma empresa a ter relacionamentos de terceiros aplicam-se à sua supervisão terceirizada: eficiência, proficiência, rigor, auditabilidade e uma perspectiva independente estão entre os principais benefícios.

Fatos relevantes

Em 2021, um grande banco foi penalizado com uma multa de US$ 1 milhão e com exigências adicionais de testes e treinamentos devido à falha em reportar adequadamente dados financeiros a um órgão regulador federal. Embora o banco tivesse contratado um prestador de serviços terceirizado para lidar com o processo, o fornecedor cometeu erros constantes que o banco não conseguiu supervisionar e corrigir adequadamente em tempo hábil.

Dados importantes

Deloitte: Pesquisa de gestão de riscos de terceiros

51%
Metade das organizações reportou um ou mais incidentes com terceiros desde o início da pandemia de Covid-19.

13%
Foram incidentes de alto impacto que comprometeram severamente o desempenho financeiro, prejudicaram o atendimento ao cliente ou violaram seriamente a regulamentação.

10%
Não tinham certeza se eles tinham sofrido um incidente com terceiros ou não.

Para obter mais informações sobre gestão de riscos de terceiros

- **Deloitte:** Pesquisa de gestão de riscos de terceiros 2021
- **Deloitte:** O desafio da gestão de riscos de terceiros
- **Wall Street Journal:** Gerencie terceiros com tecnologias de ponta

Sinais de alerta

- **Subcontratação:** Seu terceiro usa terceiros? Se, por exemplo, seu fornecedor de folha de pagamento subcontratar alguns serviços, você pode descobrir que perdeu o controle sobre os dados pessoais de seus funcionários.
- **Veneno do fornecedor:** Profissionais que reclamam sobre a confiabilidade ou o desempenho dos fornecedores externos podem ser um indicador de violações de contratos de terceiros que deveriam ser investigadas.
- **Equívocos de gestão:** A direção muitas vezes acha que pode fazer a gestão de terceiros facilmente e de forma rápida. E acha que pode fazer isso sem tecnologia. De modo geral eles não conseguem, e a organização pode ser penalizada por isso.
- **Expandindo fronteiras:** Existem muitas relações de terceiros com empresas de outras jurisdições. Se seus fornecedores operam em um ambiente com padrões regulatórios frouxos, práticas comerciais potencialmente corruptas ou uma variedade de preocupações com ESG (ambiental, social e governança), sua exposição pode exceder o seu apetite a risco.

Acertando os fundamentos

- **Envolva advogados:** A grande maioria das relações de terceiros é regida por contratos que especificam direitos e obrigações. Seu departamento Jurídico provavelmente estava envolvido na elaboração destes acordos e pode ser um recurso valioso para interpretá-los.
- **Amplie a lente:** O atual programa de gestão de riscos de terceiros realmente abrange todos as partes interessadas, ou está limitado aos fornecedores? Ele cobre todos os domínios de riscos, como anticorrupção, trabalhista, continuidade de negócios e ESG?
- **Seja proativo:** Examine o *business case* existente para suportar relacionamentos com terceiros e seu alinhamento às estratégias gerais de negócios.
- **Puxe a corrente:** Até onde a Auditoria Interna deve ir? Uma avaliação precisa de risco determinará se e quão atentamente os provedores “quarteirizados” (e além) devem ser monitorados.
- **Todo valor é relevante:** O risco não diminui proporcionalmente ao valor contratual de suas relações de terceiros. Seu risco de reputação é o mesmo com um fornecedor de R$10 mil ou com um fornecedor de R$10 milhões. Aquela pequena empresa com a qual uma organização gasta alguns milhares pode custar milhões.

Dando os próximos passos

- **Antecipe-se:** Envolva sua equipe no processo de seleção de fornecedores para vetar provedores críticos e evitar problemas potenciais antes deles chegarem.
- **Instale "portas de fogo":** Apresente recursos tecnológicos e outras abordagens de sucesso ao comitê de auditoria e outras partes interessadas. E essa é a declaração de abertura: “em vez de combater incêndios, a direção deveria instalar portas à prova de fogo."
- **Desconfie:** Antecipe maneiras pelas quais os gestores podem tentar burlar controles internos que regem as relações de terceiros. Aconselhe a gestão sobre os meios de fortalecimento.
- **Veja o lado bom:** Não apenas sinalize fraquezas em terceiros; como parte do seu trabalho, esforce-se para identificar áreas que podem demonstrar o valor adicional destes relacionamentos.
- **Traga luz às penalidades:** Determine se um processo definido existe (e se ele é seguido) para escalar as preocupações, obter recursos e cobrar penalidades por não desempenho contratual, problemas de qualidade ou outras violações.

O papel da auditoria interna

ESG (ambiental, social e governança)

Embora os relatórios obrigatórios do ESG ainda não tenham chegado em muitas jurisdições, sua adoção é iminente nas principais economias.

Nossa visão

A auditoria interna sempre esteve presente na agenda das organizações, mas agora deve ser cultivada de forma sustentável, com mão de obra justa e com emissões de carbono neutras.

Grupos de auditoria interna em grandes multinacionais podem achar relativamente indolor acomodar questões ambientais, sociais e de governança (ESG) em seus planos de auditoria interna. Mas para organizações de médio e pequeno portes, a sopa de letrinhas de padrões e frameworks do ESG – GRI, SASB, TCFD, IIRC, e muito mais – pode ser intimidante. Para esses grupos, oferecemos essa tranquilidade: você já sabe mais do que pensa. Sim, há novos requisitos, mas assim como você absorveu COSO, IFRS, FCPA, e outros padrões, você também pode lidar com isso. Fundamentalmente, a asseguração do ESG ainda é operacional e contábil, embora usando outras métricas – como galões de água, emissões de carbono e diversidade da força de trabalho.

Embora a obrigatoriedade do relatório ESG ainda não tenha chegado a muitas jurisdições, sua adoção é iminente em grandes economias. A auditoria interna não deve atrasar o endereçamento das questões, pois as apostas são simplesmente muito altas, com pressão exercida por reguladores, investidores, clientes, terceiros e a sociedade em geral. Os benefícios para acertar podem ser significativos, como "alto desempenho do ESG pode se traduzir em um melhor acesso ao capital, talentos e oportunidades de negócios."

Para funções de auditoria interna que estão apenas começando em sua jornada ESG, um desafio inicial pode ser identificar as partes responsáveis dentro da organização. Muitas vezes, encontramos o CFO apontando para a área de Relações com Investidores, que olham para o RH, que passa o bastão para o Jurídico, que redireciona para o Marketing. A coordenação efetiva entre esses grupos e a existência de um ponto focal de responsabilidade podem ser críticas para o progresso.

Fatos relevantes

As conversas sobre clima da COP26 em Glasgow levaram a acordos para eliminar a energia do carvão, reduzir as emissões de metano, deixar o setor de serviços financeiros mais verde e parar o desmatamento. No entanto, nem todos os países são signatários desses acordos, e alguns grandes emissores de CO_2 recusam-se a assinar. A adoção total, a conformidade e a responsabilização continuam sendo obstáculos significativos.

Dados importantes

- A representação feminina em conselhos corporativos varia dramaticamente em todo o mundo: Austrália-34%; Canadá-31%; França-43%; Alemanha-25%; Índia-17%; Japão-11%; Holanda-26%; Reino Unido-34%; EUA-28%.
- Líderes mundiais para métricas ESG incluem Dinamarca para desempenho ambiental, Finlândia por ausência de discriminação e Cingapura para qualidade regulatória. O Brasil não aparece atualmente no top 10 em qualquer uma dessas categorias.

Para mais informações sobre o ESG (meio ambiente, social e governança)

- **Deloitte**: Encontrar o valor no desempenho ambiental, social e de governança
- **Wall Street Journal:** ESG e o papel da auditoria interna
- **Wall Street Journal:** Cinco passos para construir compromissos climáticos confiáveis

Sinais de alerta

- **Apelo de marketing:** Se o seu departamento de marketing fizer reclamações que estão em desacordo com suas auditorias ESG, o tema precisará ser rapidamente resolvido.
- **Políticas desatualizadas:** As políticas organizacionais em torno de viagens de negócios, trabalho remoto, diversidade e inclusão, governança corporativa e muito mais devem ser revisadas e atualizadas para refletir o ambiente de negócios atual, os riscos correspondentes e as metas de ESG.
- **Um olhar detalhado:** As organizações podem estar literalmente ou figurativamente alinhadas com padrões, prioridades e exigências que variam de acordo com a geografia ou a unidade de negócios.
- **Desacordo com a estratégia:** As considerações do ESG devem ser casadas com as estratégias de negócios. Uma abordagem balanceada promoverá os objetivos da empresa; uma abordagem desarticulada pode arrastar o desempenho para baixo.

Acertando os fundamentos

- **Informe a equipe:** Familiarize sua equipe de auditoria interna com padrões e frameworks reconhecidos de relatórios ESG, como a Global Reporting Initiative (GRI), o Sustainability Accounting Standards Board (SASB), o Greenhouse Gas (GHG) Protocol e a Força-Tarefa de Divulgação Financeira Relacionada ao Clima (TFCD).
- **Verifique o status:** Analise o processo atual de divulgação de ESG para controles internos: Os controles estão funcionando e são suficientes? As descobertas foram relatadas ao conselho?
- **Ofereça dados:** Fornecer informações sobre indicadores de risco ESG ajuda a avaliar como os riscos do ESG têm sido considerados dentro do processo de gerenciamento de riscos corporativos da organização. O ESG está integrado à uma estratégia de negócios mais ampla?
- **Reveja os relatórios:** Determine como a gestão identificou os principais problemas a serem divulgados e se eles alinharam esses tópicos aos padrões reconhecidos.
- **Avalie de forma independente:** Utilize avaliações específicas e focadas para entender as políticas, as perspectivas do negócios e as responsabilidades.

Dando os próximos passos

- **Greenwashing:** Preste atenção no greenwashing. Um maior escrutínio deste tema desacelerou essa tendência, mas muitas organizações ainda fazem afirmações frágeis sobre seu perfil verde em vez de refletir sua verdadeira cor.
- **Nutrir conhecimento:** Inicie o treinamento conforme necessário para preencher lacunas de conhecimento, tanto dentro da área de auditoria interna quanto em toda organização. Planeje iniciativas de conscientização, sessões de aprofundamento em temas críticos e visões holísticas do negócio.
- **Construa credibilidade:** Atualize as qualificações da auditoria interna com certificações e credenciamentos relacionados ao ESG, obtidos por meio de organizações profissionais.
- **Financiar a equipe:** Invista em recursos com a experiência e as habilidades corretas para entender, reconhecer e avaliar os riscos do ESG. Considere criar posições dedicadas ao ESG dentro da auditoria interna para permitir conhecimento especializado e maior foco ao tema.
- **Integrar o ESG:** Inclua os riscos de ESG dentro de cada programa de auditoria interna para endereçar esses aspectos nos trabalhos aplicáveis. Considere incluir temas de ESG em seus relatórios de auditoria interna sempre que necessário.

O papel da auditoria interna

Antifraude

Uma máxima para a medicina também vale para os negócios: é melhor prevenir do que remediar.

Nossa visão

Todo país tem seu tabloide de notícias sensacionalista. E nenhuma liderança quer ver sua empresa estampada na primeira página.

Na verdade, não há maneira mais infalível de atrair publicidade indesejada do que sofrer um caso de fraude interna. Mas o dano vai muito além das manchetes espalhafatosas. A fraude prejudica não só a reputação do negócio, mas também as carreiras daqueles que assistem o ocorrido. Consequências financeiras, penalidades regulatórias, perda de clientes e ganhos de concorrentes são resultados comuns. E, em casos extremos, a fraude pode apresentar uma crise de continuidade da própria organização.

O problema permeia quase todos segmentos de negócios. Embora os serviços financeiros e o setor público estejam geralmente mais focados nesse risco, devido, em grande parte, aos rigorosos ambientes regulatórios em que operam, a maioria dos outros setores está defasada.

As *startups*, em particular, podem ter dificuldades adicionais no combate à fraude e sofrer com suas consequências.

Estranhamente, apesar da proeminência da questão, muitas organizações operam em estado de negação. Mas a postura de “se não vi, não senti” revela um fator-chave: a fraude, por sua natureza, envolve enganação. Não há luzes piscando que digam "olhe aqui“ ou “preste atenção”. Os fraudadores cobrem seus rastros e farão o possível para direcionar sua atenção para outro lugar.

Então, quando as organizações dizem: "Não temos um problema de fraude", a resposta padrão talvez devesse ser, "Sim, você tem. Você somente ainda não a identificou”.

O que é verdade na medicina também vale para os negócios: *É melhor prevenir do que remediar.* A melhor maneira de minimizar perdas de fraude é evitar que as fraudes ocorram.

Fatos relevantes

Quando a empresa alemã de tecnologia financeira Wirecard revelou que mais de US $ 2 bilhões em dinheiro tinha desaparecido de seus registros contábeis, a consequência foi rápida e severa: o preço das ações caiu mais de 90%; o CEO renunciou; a empresa entrou com pedido de insolvência; e várias pessoas executivas foram presos sob acusação de fraude contábil.

Dados importantes

De acordo com o Associação de Investigadores de Fraude Certificados:

5%

Em média, as organizações perdem 5% de suas receitas anuais por fraude.

$4.5T

Mais de US$ 4,5 trilhões são perdidos devido à atividade fraudulenta a cada ano.

14 meses

O típico caso de fraude dura 14 meses antes de ser detectado.

Para mais informações sobre combate à fraude

- **Deloitte:** A natureza da fraude está mudando
- **Deloitte:** Construindo confiança em seu quadro de risco de fraude
- **Wall Street Journal:** Cinco ações para fortalecer os planos de denunciantes

Sinais de alerta

- **Estilo de vida extravagante:** Se o assistente do contador júnior está indo para o trabalho em uma Mercedes-Benz, você deveria verificar novamente seus lançamentos contábeis. Um funcionário que vive muito além de seus meios é o sinal mais comum de atividade fraudulenta. (Pode parecer óbvio, mas ainda ocorre.)
- **Problemas pessoais:** Certas questões pessoais podem também ser um sinal de alerta antecipado para possíveis fraudes, incluindo dificuldades financeiras, divórcios e vícios. De acordo com o Associação de Investigadores Certificados de Fraude, "em 63% dos casos, o fraudador apresentou comportamento suspeito associado à sua vida pessoal."
- **Problemas de trabalho:** Alguns comportamentos no local de trabalho também podem ser indicadores adicionais de risco de fraude. Entre as principais preocupações: relações extraordinariamente próximas com fornecedores ou clientes; interações tensas entre os colegas; e avaliações de desempenho ruins.

Acertando os fundamentos

- **Compreenda o cenário:** Para obter um controle real sobre os riscos que sua organização está enfrentando, realize uma avaliação completa e abrangente do risco de fraude. Os resultados devem impulsionar as atividades subsequentes — onde se concentrar, gastar seu tempo e investir. Esse não é um exercício único de cinco minutos: fale com as partes interessadas, faça pesquisas anônimas, realize *workshops* e atualize/desafie regularmente os resultados.
- **Passe no teste:** É surpreendente quantas organizações têm lacunas ou fraquezas relevantes em controles internos essenciais. Para dissuadir a fraude, fique com o básico: segregue funções; restrinja o acesso; estabeleça limites de alçadas; realize verificações de antecedentes; alterne responsabilidades de trabalho; imponha férias obrigatórias.
- **Reforce a infraestrutura:** Estabeleça mecanismos robustos de notificação de fraudes para uso de funcionários e contratados, permitindo denúncias anônimas. Muitas vezes, esses mecanismos envolvem o uso de linhas diretas de terceiros; no entanto, é vital que os relatórios recebidos sejam analisados e as medidas de acompanhamento apropriadas sejam tomadas.

Dando os próximos passos

- **Cuidado com as lacunas:** Uma vez compreendidos os principais riscos, correlacione-os com os controles existentes para identificar lacunas, fraquezas e ações prioritárias e de ganhos rápido. Comece a fechar essas lacunas. Algumas exigirão correções de longo prazo; outras serão mais simples, sem exigir grandes investimentos.
- **Treine o time:** Com os riscos identificados e os mecanismos de notificação estabelecidos, o treinamento antifraude pode ser iniciado. Certifique-se de destacar o custo real de fraude, os sinais de alerta e os mecanismos de reporte. Comunique uma política de tolerância zero.
- **Eduque os stakeholders:** Sua melhor defesa são as partes interessadas: profissionais, gestores e terceiros. Eduque-os sobre as ameaças e os principais riscos. Ajude-os a entender como detectar e sinalizar problemas emergentes. Mas não abra completamente a porta. Mantenha informações confidenciais sobre suas melhores técnicas de detecção de fraudes em segredo.

O papel da auditoria interna

Fusões e aquisições

As negociações aumentarão na economia pós-pandemia. A auditoria interna pode ajudar as transações a ter sucesso.

Nossa visão

Executivos de M&A estão enviando sinais claros e fortes de que as transações corporativas funcionarão como uma alavanca importante à medida que as empresas se recuperam e prosperam na economia pós-pandemia. Assim como os consumidores estão reabrindo suas carteiras após a paralisação dos negócios, empresas e investidores de private equity acumularam muito capital e estão prontos para investir. Para que o negócio seja bem sucedido em longo prazo, com um foco claro no valor e no risco desde o início, a auditoria interna deve ser uma peça chave: antes, durante e depois.

Dentre as questões mais espinhosas estará a integração dos sistemas de TI. Não é incomum encontrar dezenas de sistemas de TI entre as empresas que se unem, que precisarão ser avaliados quanto à sua compatibilidade e redundância. Uma mensagem inicial de M&A provavelmente incluirá uma avaliação de sinergias potenciais, mas à medida que a data de fechamento se aproxima, esses modelos de sinergia podem diminuir repentinamente. Haverá intensa pressão para fazer as projeções iniciais funcionarem, e os sistemas de TI são frequentemente um foco de problemas.

Outra preocupação envolve processos contábeis. Durante o período do contrato de transição (TSA), os processos contábeis e de controle interno podem apresentar lacunas, resultando em problemas de relatórios financeiros potencialmente prejudiciais. Muitas empresas subestimam o esforço necessário para separar ou integrar seus sistemas contábeis. É essencial envolver as habilidades certas, em vez de apenas jogar recursos no problema.

E, finalmente, não só as lideranças de auditoria interna devem se preocupar com o esforço geral de integração, como também podem ter que lidar com a fusão de dois grupos de auditoria interna distintos. As áreas precisarão conciliar diferenças de visão, foco e função, modelos operacionais, documentação de papéis de trabalho, ferramentas e tecnologia e muito mais. Essa integração não pode ser uma questão de retrocesso: uma vez que a auditoria interna estará aconselhando sobre a integração dos negócios, é essencial para a manter credibilidade que tenha sua própria casa em ordem. Começar cedo e se mover rapidamente são as chaves para o sucesso.

Fatos relevantes

Em 2001, a America Online fundiu-se com a gigante Time Warner na expectativa de criar um grande conglomerado de mídia. Mas sinergias não exatamente realizadas, culturas conflitantes e uma bolha de internet estourando levaram a AOL/Time Warner a sofrer uma perda de quase US$ 99 bilhões em 2002, ganhando o título de "a pior fusão de todos os tempos." Embora o acordo seja de mais de vinte anos atrás, os aprendizados ainda se aplicam.

Dados importantes

De acordo com a pesquisa da Deloitte 'Futuro e Tendências de M&A":

61%

dos negociadores dos EUA esperam que a atividade de M&A retorne aos níveis pré-Covid-19 até o final de 2022.

51%

As ameaças à segurança cibernética são prioridade para 51% dos entrevistados, à medida que as empresas gerenciam negócios virtualmente.

Condições incertas de mercado, traduzir as necessidades estratégicas dos negócios em uma estratégia de M&A e a valorização dos ativos são considerados os maiores desafios para o sucesso de M&A.

Para mais informações sobre fusões e aquisições

- **Deloitte:** Pesquisa de tendências de M&A: O futuro da M&A
- **Deloitte:** M&A: A intersecção de due diligence e governança
- **Deloitte:** Realidades regulatórias em meio ao impulso do mercado de M&A

Sinais de alerta

- **Incompatibilidades básicas:** Organogramas verticais *versus* horizontais. Tomada de decisão metódica *versus* não estruturada. Liderança conservadora *versus* arrojada. Alguns obstáculos culturais podem ser importantes demais para pular.
- **Lógica insuficiente:** Alcançar economias de escala é frequentemente citado como um motor de negócios de M&A, mas se você fundir duas empresas com estratégias defeituosas, má liderança ou concorrência implacável, a única coisa que você estará escalando é a probabilidade de fracasso.
- **Problemas de ESG:** A empresa adquirida tem um histórico irregular de ESG? O acordo vai fazer com que seu próprio programa ESG retroceda em vários anos?

Acertando os fundamentos

- **Faça due diligence:** À medida que os negócios potenciais são avaliados, a auditoria interna deve garantir que todas as áreas prioritárias sejam cobertas; avaliar o ambiente de controle interno existente; e revisar questões materiais de auditorias recentes.
- **Encontre sinergias:** Os negociadores às vezes apresentam um quadro excessivamente otimista de sinergias potenciais. Dê uma olhada independente e reporte as descobertas ao conselho. Acompanhe por um ano ou mais o cenário pós-transação para ver onde está e não está sendo identificada a sinergia.
- **Envolva a auditoria interna:** A auditoria interna deve participar das sessões de planejamento, focando sua lente de risco e controle e fazendo perguntas difíceis. Em alguns negócios, a auditoria interna pode ser excluída do projeto, mas uma vez que o acordo é anunciado, a função deve pressionar para ser envolvida.
- **Atividades prioritárias:** A auditoria interna tem uma visão única e ampla da organização – quem é quem, como a empresa está conectada, onde a nova empresa se encaixa. Esse conhecimento deve ser utilizado como parte do planejamento e suporte, com prontidão desde o 1º dia.

Dando os próximos passos

- **Compare e aconselhe:** Verifique processos, monitoramentos e tecnologia na empresa-alvo. Identifique estados atuais; mapeie sinergias e determine redundâncias; identifique o que é coberto pelo acordo de transição.
- **Encontre a saída:** Examine o TSA e recomende mudanças conforme necessário. Acompanhe as datas finais do TSA e avalie como a empresa está se preparando para uma saída oportuna sem estender o acordo de transição para cobrir as deficiências.
- **Olhe para trás:** Realizar avaliações pós-transação para verificar lições aprendidas que podem ser aplicadas a outros negócios, daqui para frente.
- **Contemple o compliance:** Se o acordo empurrar a empresa adquirente para novos mercados, outros requisitos adicionais de regulação e reporte entrarão em jogo. Avalie cedo para evitar o não cumprimento e prazos perdidos e as dores de cabeça que eles trazem.

O papel da auditoria interna

Segurança psicológica

O velho ditado, “segurança em primeiro lugar", ganha um novo significado para a auditoria interna.

Nossa visão

Afirmar que os ambientes de trabalho devem abraçar colaboração e o aprendizado tornou-se um clichê de negócios, mas na verdade existem dados concretos para apoiar essa afirmação. Um estudo de dois anos sobre o desempenho de equipes conduzido pelo Google revelou que os times de melhor desempenho tinham adotado o conceito de "segurança psicológica" — a noção de que os erros são precursores do sucesso e que aqueles que os fazem devem ser apoiados, não punidos. O Google concluiu que quando as equipes têm liberdade de se envolver em riscos estratégicos em um ambiente de apoio, sua confiança coletiva, criatividade e produtividade aumentarão.

O estudo do Google é convincente, mas antes de a auditoria interna começar a defender a segurança psicológica para toda organização, é preciso olhar para si mesma. O grupo de auditoria interna está contribuindo de forma positiva ou negativa para os níveis de segurança psicológica na organização? Para determinar a resposta, comece com uma pesquisa de perguntas simples às áreas auditadas: "*Como se sente ao ser auditado por nós?*“

As respostas podem vir como um choque: para a maioria dos auditados, passar por uma auditoria interna é semelhante a um teste médico invasivo – necessário e importante, talvez, mas detestado e temido.

Para a auditoria interna, então, a segurança psicológica começa em casa. Tome medidas para tornar sua função menos parecida com um adversário, e mais próxima a um conselheiro. Não apenas destaque o que está ruim, mas também celebre o bom. Não apenas escrutine o passado, mas vislumbre o futuro.

Para promover a segurança psicológica, as equipes de auditoria interna podem adotar uma declaração conhecida como "A Primeira Diretriz": "Independentemente do que descobrirmos, entendemos e realmente acreditamos que todos fizeram o melhor trabalho que puderam, dado o que sabiam na época, suas competências e habilidades, os recursos disponíveis e a situação em questão.” (Norm Kerth, Project Retrospectives: A Handbook for Team Review)

Histórico relevante

No início de sua carreira, o inventor americano Thomas Edison foi demitido pela Western Union depois que um experimento fracassado danificou a propriedade da empresa. A rescisão foi feita de forma imediatista por parte de seu empregador, já que Edison passou a registrar mais de mil patentes, inventando a lâmpada elétrica, toca-discos, câmera de cinema e muitos outros dispositivos. Anos mais tarde, a Western Union, depois de negligenciar a criação de um ambiente de trabalho onde era seguro falhar, acabou comprando os direitos de uma das invenções de Edison.

Dados importantes

- A pesquisa Auditoria Interna 2020 da Deloitte revelou que 86% dos coordenadores de comitês de auditoria e conselheiros disseram que a administração é encorajada a apresentar problemas e conclusões ao comitê de auditoria, mas as barreiras institucionais muitas vezes impedem que isso aconteça.
- Uma pesquisa global de auditoria interna da Deloitte em 2018 revelou que apenas 33% de pessoas executivas de auditoria acreditavam que sua função de auditoria interna era vista de forma muito positiva.
- O site Internal Audit 360 descobriu que os relatórios de auditoria interna "não costumam comunicar os aspectos positivos do ambiente de controle interno e governança."

Para mais informações sobre segurança psicológica

- **Deloitte:** Otimização da auditoria interna: Desenvolvimento de equipes de primeira linha
- **Deloitte:** Criando resiliência através da segurança psicológica
- **New York Times:** O que o Google aprendeu com sua busca para construir a equipe perfeita

Sinais de alerta

- **Executivos ríspidos:** Se seus relatórios de auditoria provocarem erupções na liderança e “tremores nas equipes”, pode ser seguro supor que a segurança psicológica ainda não tenha sido alcançada em toda a organização.
- **Olhares desviados:** Falta de uma postura amistosa ou de bom relacionamento entre auditoria interna e unidades de negócios pode ser um sinal de que as relações estão tensas, fazendo um ambiente de segurança psicológica mais difícil de estabelecer.
- **Missão mal interpretada:** Se o propósito percebido da auditoria interna (dentro e fora da função) é "fornecer segurança e aconselhamento", ao invés de "ajudar a organização a ter sucesso", então a base sobre a qual a segurança psicológica é estabelecida necessita de ajustes.

Acertando os fundamentos

- **Audite a si mesmo:** Pergunte às partes interessadas como é ser auditado. Se as pessoas auditadas acharem suas auditorias inapropriadas ou desconfortáveis, ou se o perceberem mais como polícia e menos como conselheiro, ajustes são necessários.
- **Cuidado com o tom:** Analise o tom que você usa em relatórios para o nível executivo e o comitê de auditoria. Quão útil ele é para facilitar bons resultados e criar um ambiente positivo? Considere reformulações para evitar linguagem emotiva e acusatória.
- **Influenciar os influenciadores:** Identifique partes interessadas influentes e converse com eles sobre possíveis passos para criar um ambiente onde as pessoas tenham uma resposta positiva às auditorias. Como os temas críticos e ásperos podem ser melhor endereçados?

Dando os próximos passos

- **Renove os relatórios:** Esforce-se para contar melhor a história. Considere separar as questões do ambiente de controle do resto do relatório, reconhecendo que um ambiente de controle ruim pode ser uma anomalia temporária devido a fatores como implementação de novos processos ou expansão para um novo mercado ou país.
- **Destaque o positivo:** Celebre comportamentos positivos tanto dentro de seus relatórios e por meios separados, como boletins informativos internos ou outras formas de reconhecimentos. Tais ações não só beneficiam os destinatários, mas também iluminam um pouco a própria auditoria interna.
- **Ajude a mudar a visão do comitê de auditoria:** Como principal consumidor dos relatórios de auditoria interna, o comitê de auditoria possui um papel fundamental na habilitação da segurança psicológica: liderar pelo exemplo, definir o tom e responder aos resultados da auditoria como uma oportunidade de aprendizado e melhoria, em vez de ser uma ocasião para críticas e repreensões.

O papel da auditoria interna

Cibersegurança

Tecnologia emergente é igual a ameaças emergentes.

Nossa visão

P: Qual é o maior receio da auditoria interna sobre segurança cibernética?

R: Tudo o que a liderança acha que está sob controle.

A preocupação da equipe de auditoria interna é bem justificada. Aqui está uma lista abreviada de temas que a gerência normalmente subestima:

- Quantos ex-funcionários ainda possuem usuários ativos no ERP
- Número de fornecedores terceirizados com acesso aos sistemas de TI
- Quantidade de processos em nuvem que a empresa utiliza
- Total de violações cibernéticas que a empresa sofreu

Ao corrigir esses equívocos, as lideranças de auditoria interna devem ter atenção especial aos seguintes pontos:

Nuvem: A complexidade aumenta à medida que as empresas terceirizam serviços em nuvem, aumentando sua dependência de terceiros (ex.: risco de cadeia de suprimentos) e ampliando sua exposição aos ataques. É preciso aumentar os conhecimento dos auditores internos sobre riscos específicos de ambientes em nuvem para endereçar adequadamente esses aspectos. Embora a nuvem aumente a capacidade de aproveitar rapidamente novos recursos, como inteligência artificial, machine learning e blockchain, esses serviços também trazem um conjunto de riscos mais complexos.

Considere abordagens como estratégia de migração em nuvem com base em riscos, aproveitamento dos recursos nativos dos provedores e incorporação de segurança multi-nuvem. Para a auditoria interna de TI, a asseguração de nuvem será uma jornada de vários anos – não uma avaliação pontual.

Privacidade: Com reguladores e investidores aumentando a pressão, a privacidade deve estar no radar dos executivos de auditoria interna. Inicialmente, a auditoria interna precisa entender quais são os dados críticos e onde são armazenados para, em seguida, avaliar os riscos com a gestão: precisamos e usamos todas as informações pessoais identificáveis (IPI) que coletamos? Será que todos que têm acesso aos dados realmente precisam disso? Temos salvaguardas suficientes para proteger as IPIs? Temos processos de descredenciamento para ex-funcionários? Como o trabalho remoto impactou a privacidade dos dados?

Talentos: Atrair e reter especialistas em segurança cibernética é um desafio significativo para a auditoria interna, mas vencer a guerra de talentos é um imperativo. Ao conversar com a equipe de tecnologia sobre seus sistemas e controles, os auditores internos de TI que não têm “credibilidade" serão naturalmente preteridos por não agregarem valor. Algumas soluções para a crise de talentos podem ser encontradas em oportunidades de treinamento, redirecionamento de carreira ou terceirização de auditoria interna de TI para terceiros respeitáveis.

Fatos relevantes

Apesar da divulgação ampla e frequente de vazamentos de dados, notícias abrangem apenas uma fração dos ataques cibernéticos. De acordo com a revista Security "mais da metade dos empresários admite esconder um vazamento de dados."

Dados importantes

43% De ataques cibernéticos têm como alvo pequenas e médias empresas.

64% Das empresas sofreram ataques com base na web.

9,7 M Registros de saúde foram comprometidos somente em setembro de 2020.

75B Em 2025, 75 bilhões de dispositivos de Internet das Coisas (IoT) estarão on-line.

Para obter mais informações sobre segurança cibernética

- **Deloitte:** Cibersegurança e o Papel da Auditoria Interna
- **Deloitte:** Garantia na Nuvem
- **ISACA:** Cloud Computing para Auditores

Sinais de alerta

- **Silêncio cibernético:** Se o seu grupo de TI não reportou nenhuma tentativa de ataque cibernético, o problema pode ser a falta de capacidade de detecção, em vez da ausência de hackers.
- **Controle de nuvem:** Se sua estratégia de migração atual de nuvem não envolveu padrões de mercado ou avaliação de um catálogo de riscos para uso destes serviços, você pode estar deixando riscos sob a mesa, em áreas onde a organização tem responsabilidade de implementar controles para restringir o acesso do usuário, personalizar interfaces ou criptografar dados, potencializando problema de controle e segurança em nuvem.
- **Domínios indefinidos:** Deve existir uma delimitação clara de responsabilidades entre o provedor de serviços em nuvem e o cliente, e isso muitas vezes envolve temas complexos. A falta de definições claras pode dar uma falsa sensação de segurança às partes interessadas.

Acertando os fundamentos

- **Treine:** Avalie as habilidades em nuvem e segurança cibernética existentes na equipe de auditoria interna. Aborde as lacunas por meio de recrutamento, treinamento e/ou terceirização, conforme necessário. Considere abordagens criativas para atrair e reter funcionários valiosos.
- **Estabeleça um framework:** Defina um programa de trabalho holístico e com base em riscos, construído sobre uma nuvem testada e estrutura de segurança cibernética. Usando esses padrões como guia, ofereça serviços de asseguração e aconselhamento para medir as capacidades cibernéticas e a maturidade da organização.
- **Indicadores dos provedores:** Antes de se estabelecer em um provedor de nuvem, solicite evidências de resiliência de infraestrutura, tempo de inatividade do serviço, desempenho e outras métricas. Revise o relatório de sistemas e controles (ex.: SOC), se disponível. Questione sobre conformidade regulatória e avaliações independentes de controles. Observe red flags e busque remediações ou alternativas, quando necessário.

Dando os próximos passos

- **Abrace o futuro:** Amplie seu plano de auditoria para englobar riscos emergentes, incluindo TI e governança de dados; questões de gestão de mudanças em sistemas e plataformas; infraestrutura terceirizadas de TI; e novas tecnologias como Inteligência artificial, RPA, *blockchain*, realidade virtual e aumentada e IoT.
- **Prepare-se:** Dado o aumento de ataques cibernéticos e perdas de dados, e as expectativas crescentes dos reguladores, é fundamental para a auditoria interna entender os riscos cibernéticos e se preparar para as perguntas e preocupações expressas pelo comitê de auditoria e pelo conselho.
- **Cruze a fronteira:** Os requisitos regulatórios em torno da privacidade dos dados variam de acordo com a jurisdição. Realize uma revisão abrangente que considere todas os segmentos e geografias de operação – físicas e virtuais – em relação às leis e regulamentos locais.

O papel da auditoria interna

Diversidade, igualdade e inclusão

A auditoria interna tem a oportunidade e a obrigação de fomentar uma cultura diversa e inclusiva.

Nossa visão

Historicamente, a auditoria interna tem sido principalmente uma operação bastante objetiva, com foco em dados rígidos e resultados mensuráveis, afastando-se de questões qualitativas que carecem de KPIs distintos. Esses dias acabaram.

Os eventos e as tendências atuais – incluindo ações de combate ao racismo, da injustiça e da desigualdade – empurraram a auditoria interna para um novo patamar de diversidade, igualdade e inclusão (DE&I). Enquanto isso representa uma área não tradicional para esta atividade, inúmeros fatores – elevados e pragmáticos – obrigam a auditoria interna a fazer um balanço das iniciativas de DE&I em toda a organização e desempenhar um papel na promoção dessas ações:

- Práticas discriminatórias são inerentemente censuráveis. A auditoria interna tem a oportunidade e a obrigação de ajudar a organização a fomentar uma cultura diversa e inclusiva.
- Uma força de trabalho diversificada e uma cultura inclusiva são componentes essenciais de organizações bem sucedidas, correlacionadas com melhor desempenho no trabalho, retenção de talentos e diminuição do absenteísmo.
- Diversidade, igualdade e inclusão são atributos críticos para candidatos a trabalho, e organizações que abraçam a DE&I terão uma vantagem em recrutar os melhores talentos.

A auditoria interna, com sua ampla perspectiva sobre riscos e suas relações abrangentes a toda organização, é bastante adequada para ajudar as organizações a avaliarem seu estágio atual de DE&I, aconselhando sobre eventuais lacunas e caminhos apropriados para aprimoramento. Isso inclui servir como catalisadores, aconselhando indicadores de riscos e KPIs; avaliar se os programas de DE&I estão cumprindo seus objetivos; e reportando resultados ao conselho, comitês e líderes sêniores.

A auditoria interna deve estar atenta – e aconselhar – contra quaisquer soluções rápidas ou rasas propostas ou promulgadas pela administração. Se a iniciativa de DE&I parecer uma abordagem paliativa, os funcionários e o mercado notarão rapidamente.

Fatos relevantes

Em 2018, um tribunal do Reino Unido decidiu que uma empresa de marcas de luxo tinha um "ponto cego sobre raça". Em um caso de discriminação trazido por um empregado, o tribunal trabalhista de Londres citou múltiplas afrontas da empresa, incluindo um processo de recrutamento tendencioso, treinamento inadequado de igualdade e diversidade, e vigilância secreta injustificada de seus profissionais.

Dados importantes

Em uma pesquisa da Deloitte de 2019, 64% dos entrevistados disseram que tinham experimentado ou testemunhado vieses no local de trabalho nos 12 meses anteriores, sugerindo uma fraqueza significativa na cultura de muitas organizações. No entanto, aproximadamente 70% dos grupos de auditoria interna não avaliam a cultura organizacional como parte de seu plano de auditoria.

Para mais informações sobre diversidade, igualdade e inclusão

- **Deloitte:** O imperativo de inclusão para os conselhos
- **Wall Street Journal:** O papel da auditoria interna na condução da diversidade, inclusão
- **Wall Street Journal:** Diversidade de conselhos melhora, mas objetivos-chave a décadas de distância

Sinais de alerta

- **Demissões rasas:** As demissões e as razões por trás delas podem oferecer pistas sobre se existem problemas de diversidade ou inclusão. Se as causas básicas das demissões revelarem um padrão, avalie para questões culturais subjacentes.
- **Boato social:** Postagens negativas em ferramentas de recrutamento ou mídias sociais podem ser um prenúncio de problemas de DE&I. Recursos para monitoramento e soluções automatizadas (próprias ou de terceiros) podem trazer informações úteis para que a organização possa estar atenta às tendências e exceções.
- **Demografia condenatória:** Os dados demográficos da sua organização podem demonstrar um viés ou práticas discriminatórias. Analisar a composição da diretoria, estilo de liderança no C-level; práticas de contratação, promoção e rescisão; aumentos de salário, bônus e benefícios e outras métricas podem revelar pontos de fragilidade.

Acertando os fundamentos

- **Comece pequeno:** Desenvolva uma avaliação de cultura para determinar a existência e o escopo das iniciativas de DE&I. Documente o que sua organização está fazendo atualmente para entender, comunicar e moldar sua cultura corporativa.
- **Incorporar riscos:** Inclua riscos de DE&I em seu plano de trabalho. Avalie as iniciativas atuais para determinar se elas estão cumprindo seus objetivos. Informe as partes interessadas sobre as oportunidades de melhoria e o progresso de DE&I em cada relatório de auditoria.
- **Auxilie e incentive:** Ajude a liderança a entender as implicações de uma cultura organizacional insalubre vista através de uma lente de risco. Forneça informações sobre treinamento, comunicações e políticas.
- **Faça perguntas:** Para entender as percepções e experiências dos profissionais e identificar potenciais riscos, desenvolva, como parte do plano de auditoria, um questionário padrão para orientar entrevistas com as partes interessadas. Realize entrevistas com uma amostragem diversificada dos colaboradores.

Dando os próximos passos

- **Facilitar a melhoria:** Avalie os métodos utilizados para monitorar, medir e relatar o programa e avaliar se alguma melhoria pode ser feita.
- **Validar estatísticas:** Se sua organização publicar estatísticas de DE&I no mercado, forneça asseguração sobre precisão e controles.
- **Ferramentas e tecnologia:** Aproveite ferramentas e tecnologias inovadoras, como risk sensing, para avaliar problemas de DE&I e identificar riscos potenciais.
- **Reconciliar realidades:** A auditoria interna pode ser bastante efetiva ao desenvolver recomendações para diminuir a distância entre percepções de liderança e realidades dos funcionários na cultura corporativa.

O papel da auditoria interna

Asseguração no design

Para transformações ou implementações, os controles devem ser premeditados, não uma reflexão posterior.

Nossa visão

Se você gastou mais de um milhão por uma Lamborghini, você certamente tiraria pleno proveito de seu enorme motor de 12 válvulas, sua aceleração de força G, e sua multiplicidade de sensores e alertas automatizados.

No entanto, o mesmo não pode ser dito para organizações que investem somas relevantes para sistemas corporativos (ERP). Em nossa experiência, uma ampla gama de recursos e controles internos no âmbito destes sistemas são insuficientemente validados e implementados, ou não são utilizados da melhor forma. É o equivalente a comprar um carro esportivo italiano e nunca tirá-lo da segunda marcha.

Recuperar os valores investidos em sistemas ERP começa muito antes da sua utilização. Envolve principalmente a adoção de uma mentalidade consciente dos profissionais envolvidos para gerenciar efetivamente os riscos operacionais e estratégicos em toda a organização.

Ou seja, ao invés de considerar o sistema ERP como um simples meio de gerenciar eficientemente o RH, os estoques, as finanças, os clientes ou a cadeia de suprimentos, a organização deveria olhar para ele também como uma ferramenta poderosa para auxiliar na gestão dos diversos riscos associados a essas atividades.

A consciência sobre a importância de controles nas implementações e transformações da empresa começa com o alinhamento sobre a natureza e escopo das atividades realizadas pelas estruturas de apoio à governança (3 linhas), permitindo navegar de forma eficiente pelos riscos e garantir que não haja lacunas. Isso envolve uma interação adequada entre as áreas de negócios da primeira linha, profissionais de gestão de risco e conformidade de segunda linha e os auditores internos. Esse exercício de coordenação/colaboração não deve ser feito superficialmente, pois é a base sobre a qual uma implantação ou atualização de ERP bem-sucedida será construída.

Fatos relevantes

Em uma auditoria de 2018 em uma agência do governo dos EUA, quase metade das deficiências citadas estavam relacionadas aos seus sistemas de TI. Dentre as diversas descobertas, os auditores observaram que a agência não tinha implementado controles de segurança destinados a detectar alterações acidentais ou não autorizadas nos dados financeiros.

Dados importantes

Em uma pesquisa recente da Deloitte, quase metade da liderança disse que as implementações de tecnologia – incluindo ERP, automação, migração em nuvem e controles relacionados ao trabalho remoto e outros riscos associados – levarão suas organizações a remediar processos financeiros no próximo ano.

Para mais informações sobre asseguração no design

- **Deloitte:** Garantia por design: Elaborando o manual de controle para transformações
- **Deloitte:** Modernização das três linhas do modelo de defesa
- **Wall Street Journal:** Garantia por design – considere as necessidades de controle na frente

Sinais de alerta

- **Módulos mal aproveitados:** Um número surpreendente de organizações não consegue tirar proveito dos controles robustos incorporados nos seus sistemas ERP. Ambientes de controle que dependem fortemente de controles manuais podem ser mais suscetíveis a atrasos, erros e fraudes.
- **Custos de escalada:** Seus custos pós-implementação podem ser significativamente maiores se os controles e a garantia associada não forem adequadamente considerados e antecipados.
- **Atribuição clara de responsabilidades:** Confusão e ineficiências podem reinar se as equipes de segunda e terceira linha estiverem pisando nos pés dos outros ou não estiverem claras sobre quem está fazendo o quê.

Acertando os fundamentos

- **Conecte-se:** Aproxime-se dos amplos grupos de trabalho e outros *stakeholders* em toda empresa para ajudar a identificar os recursos necessários para processos de negócios e controles mais eficientes.
- **Compartilhe sabedoria:** Aconselhe a liderança a considerar não apenas os riscos financeiros e de conformidade, mas também os riscos operacionais, cibernéticos e estratégicos, que envolvem um conjunto mais amplo de controles e capacidades necessárias para alcançar os objetivos de negócios.
- **De olho nas modernizações:** Identifique oportunidades para automatizar ou modernizar controles, aumentando a eficiência, reduzindo erros e automatizando os trabalhos de asseguração.

Dando os próximos passos

- **Use sua expertise:** Se sua organização estiver considerando uma implementação transformadora de projetos ou sistemas, certifique-se de que os donos dos controle e processos reflitam e estejam conscientes sobre os riscos envolvidos, desde o início.
- **Alinhe com a estratégia...:** Aproveite para alinhar suas três linhas de defesa, esclarecendo papéis e responsabilidades. Diminua eventuais tensões e evite disputas de território. Pense em todos os passos e atividades.
- **... e auditores:** Desenvolva uma metodologia e uma estratégia detalhada sobre como os controles são considerados e validados durante a implementação. Esteja totalmente alinhado com os auditores externos para evitar surpresas após a implementação.
- **Pense nas pessoas, não apenas nos controles:** Olhe para a capacitação das equipes responsáveis pelo controle. Isso envolve treiná-las sobre o que elas precisam fazer após o go-live do ERP, para atender aos requisitos de conformidade.

O papel da auditoria interna

Bullying e assédio

A cultura tóxica emergiu como a causa-raiz de falhas relevantes nas organizações. A auditoria interna pode ajudar a melhorar o ambiente.

Nossa visão

Dada a preponderância do assédio no local de trabalho e histórias de bullying nas notícias, ficamos curiosos: Por que mais empresas não saem à frente nesta questão?

As desculpas eram tão variadas quanto equivocadas:

1. "Se houver uma provocação no tema, você vai ter excesso de reclamações e relatos."
2. "Tivemos alguns casos, sem relação entre si, que não são refletem nossa cultura corporativa global."
3. "Temos um código de conduta de longa data que nos protege."

A Auditoria interna tem um papel significativo a desempenhar no apoio às empresas que levam o risco de cultura à sério, minimizar a ocorrência desses equívocos. O objetivo da auditoria interna não é ser um moralizador, árbitro, ou xerife, mas sim atuar como facilitador, observador e conselheiro.

O risco cultural pode ser avaliado comparando dados de várias fontes, incluindo pesquisas, entrevistas, grupos focais, ferramentas de sensoriamento de riscos, análises e programas de conformidade/conduta. Analisar uma combinação de fontes qualitativas e quantitativas permite construir um quadro amplo e mais claro para antecipar e mitigar os diversos tipos de problemas potenciais.

Os benefícios de abordar proativamente questões culturais podem ser múltiplos. Por exemplo, em um ambiente onde a concorrência por talentos de ponta é feroz, organizações que constroem um ambiente positivo, solidário e confiável, que permite que os funcionários prosperem, atrairão e reterão os trabalhadores mais desejáveis. Em última análise, uma cultura positiva no local de trabalho favorece muito a realização de objetivos organizacionais. Por outro lado, as organizações que não conseguem cultivar tal cultura podem incorrer em repercussões reputacionais, regulatórias, legais e financeiras significativas.

Fatos relevantes

Em 2021, o governador de Nova York Andrew Cuomo renunciou ao cargo em meio a uma investigação de assédio sexual, após acusações feitas por quase uma dúzia de mulheres. Uma investigação descreveu o ambiente de trabalho no gabinete do governador como "extremamente tóxico, extremamente abusivo."

Dados importantes

86%

De executivos pesquisados em todo o mundo afirmam que a cultura organizacional é "muito importante" ou "importante".

12%

De empresas acreditam que suas organizações estão impulsionando a "cultura certa".

Para mais informações sobre bullying e assédio

- **Deloitte:** Cultura e conduta no local de trabalho: desafios e oportunidades
- **Deloitte:** Projetando trabalho para o bem-estar
- **Wall Street Journal:** O bem-estar pode oferecer retornos saudáveis

Sinais de alerta

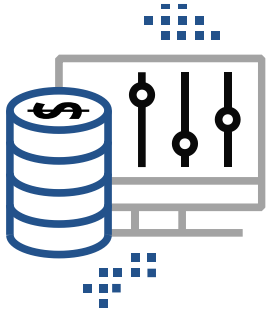
- **Silêncio ensurdecedor:** Um sinal de alerta pode não ser tão evidente. Funcionários podem ter ficado em silêncio porque queixas anteriores não foram consideradas. Outros problemas de comunicação: medo de retaliação; processos de denúncias complicados; dificuldades para reunir provas.
- **Seca de talentos:** Se você observou um aumento de atritos ou uma contratação lenta, questões culturais podem estar relacionadas.
- **Ruído de fundo:** Comentários negativos em redes sociais e sites de busca de emprego podem ser precursores de crises completas, que muitas vezes se estendem às mídias e tribunais.
- **Panela de pressão:** Organizações que exercem pressão implacável em torno de lucros trimestrais e metas de vendas podem estar criando um ambiente que potencializa o assédio e o bullying. O comportamento abusivo é frequentemente correlacionado com demandas de desempenho irrealistas ou inatingíveis.

Acertando os fundamentos

- **Faça um balanço:** Faça um inventário e revise códigos de ética, programas antifraude, políticas e procedimentos de má conduta e linhas diretas ou mecanismos alternativos de emissão de relatórios de olho na pontualidade, clareza, relevância e exequibilidade.
- **Traga o assunto para a pauta:** Incentive o conselho e o comitê de auditoria a adicionar a cultura do trabalho como tema recorrente às suas agendas.
- **Integre:** Considere quem está no comando das questões culturais. Muitas vezes a responsabilidade é fragmentada entre RH, jurídico, compliance e unidades de negócios. Às vezes, uma equipe levanta preocupações, outra investiga, e o resto da organização é deixada no escuro. Torne-se um facilitador da união e da convergência das ações.

Dando os próximos passos

- **Consulte:** Aconselhe a gestão sobre o estabelecimento de um quadro de avaliação de riscos culturais que forneça *insights* sobre cultura organizacional, engajamento e comportamentos dos funcionários e sinais de mercado.
- **Avalie e meça:** Adicione trabalhos de asseguração em aspectos culturais ao plano de auditoria. Estabeleça, monitore e informe métricas relacionadas à conduta dos funcionários e violações éticas e garanta que os níveis executivos e de conselho revisem tais dados.
- **Incentive:** Recomende o realinhamento do pagamento pelo desempenho e revisão de como os incentivos salariais impulsionam o comportamento.
- **Evangelize:** Estimule comunicações frequentes e treinamento abrangente sobre questões culturais.
- **Reporte:** Seus relatórios de auditoria sobre cultura não precisam de "nome e sobrenome", mas podem enquadrar a discussão em torno de dados e tendências: "No último período de seis meses, tivemos X número de relatos, dos quais Y foram comprovados, representando uma diminuição de Z por cento em relação ao período anterior. As ações proativas da gestão que contribuíram para a melhoria desse quadro foram..."



O papel da auditoria interna

Controles financeiros

A SOx do Reino Unido está no horizonte, com União Europeia, África, Austrália e outras regiões prontas para seguir o exemplo.

Nossa visão

Uma vez que as empresas dos EUA superaram o choque inicial da Lei Sarbanes-Oxley (SOx), de 2002, muitos abordaram a regulamentação não apenas como um requisito de conformidade, mas como uma chance de trazer melhorias transformadoras em seus controles internos sobre relatórios financeiros. A chegada iminente do equivalente britânico, apelidado de "SOx do Reino Unido", oferece às empresas que têm negócios no Reino Unido a mesma oportunidade.

As atividades necessárias para cumprir – e ir além das questões regulatórias – impactarão grande parte da organização. Felizmente, as lições aprendidas com a legislação norte-americana podem ajudar na aplicação destes padrões no Reino Unido e outras localidades. Algumas das vantagens para auditoria interna e a organização em geral são:

- A SOx do Reino Unido provavelmente será introduzida em 2023/24. Não importa quanto tempo você acha que tem que se preparar, não será suficiente. **Comece a planejar agora.**
- Quando promulgada, espera-se que a Sox do Reino Unido esteja entre os mais altos padrões mundiais de controle interno sobre relatórios financeiros (ICFR). Mesmo que sua organização não opere no Reino Unido, **aderir a esses requisitos rigorosos** faz sentido para os negócios.
- Com a chegada da UK SOx, a demanda por talentos será intensa, com as maiores empresas rapidamente sugando recursos. Organizações de médio e menor porte devem **reter seus talentos** agora para não serem prejudicadas.
- Novos controles podem ser necessários para cumprir com a lei britânica, mas na era pandêmica também poderá ser necessário **revisitar controles que perderam rigor** decorrente das rápidas mudanças para viabilizar trabalho remoto.
- Desde que o a lei norte-americana foi promulgada em 2002, avanços significativos foram feitos em **controles digitais**, que deverão ser considerados para alavancar a lei britânica equivalente.
- O comitê de auditoria e a equipe executiva têm papéis críticos na implementação dos requisitos regulatórios. Aqueles que tiveram experiência anterior vão conseguir; os outros vão **precisar de apoio especializado.**
- Algumas organizações farão apenas o mínimo necessário para cumprir. Outros irão **aproveitar o momento** como uma oportunidade de melhoria transformadora. Nós escrevemos sobre essas empresas de vanguarda no Harvard Business Review em 2006.

Fatos relevantes

Em 2019, a Comissão de Valores Mobiliários dos EUA (SEC) cobrou quatro empresas de capital aberto sobre a falta de manutenção dos controles internos sobre relatórios financeiros (ICFR), envolvendo vários relatórios anuais. As consequências do fracasso incluíram penalidades financeiras, requisitos de remediação e danos à reputação.

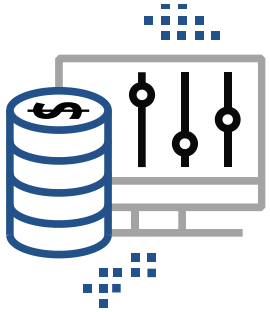
Dados importantes

1400

Em 2017, quase 1.400 empresas de capital aberto nos EUA relataram fraqueza material no ICFR.

80%

De acordo com um estudo de 2013 do US Government Accountability Office, 80% das empresas pesquisadas viram o requisito do atestado de auditor da SOx como benéfico para a qualidade dos controles da empresa.



Para mais informações sobre controles financeiros

- **Deloitte:** Considerações para auditoria interna à luz da UK SOX
- **Deloitte:** O futuro dos controles
- **GOV.UK:** Restaurando a confiança na auditoria e na governança corporativa

Sinais de alerta

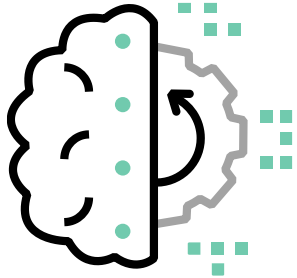
- **Auditorias pouco relevantes:** Se a auditoria externo descobriu recentemente fraquezas materiais ou deficiências significativas, ou se sua organização foi forçada a reavaliar demonstrações financeiras previamente emitidas, você pode ter algum trabalho a fazer para estar pronto para estes novos padrões.
- **Trabalho manual:** Processos financeiros que dependem fortemente de entradas de dados e controles manuais normalmente possuem maior probabilidade de erro do que sistemas automatizados.
- **Nova (e antiga) tecnologia:** A implantação de novos sistemas ERP (Enterprise Resources Planning), CRM (Customer Relationship Management), e outros sistemas de tecnologia podem criar novos riscos para o ICFR. Sistemas de TI mais antigos também podem não ter controles suficientes.
- **Partidas e chegadas:** A saída de pessoas sêniores dos setores financeiros e contábeis pode muitas vezes precipitar uma fraqueza no ambiente de controle. E fusões ou aquisições recentes ou pendentes apresentarão novos desafios a serem enfrentados.

Acertando os fundamentos

- **Avalie as áreas:** Realize uma avaliação de risco financeiro e de fraude para definir o perímetro, para mostrar a amplitude das áreas que provavelmente estarão no escopo para mapear processos e identificar riscos prioritários e controles internos chave.
- **Defina bem:** Escolha uma área e um representante para entender tanto o que é bom quanto as prováveis demandas de recursos adicionais para um projeto de conformidade ICFR de escopo completo.
- **De olho na TI:** Confirme quais os sistemas de TI no escopo. A não identificação de sistemas no escopo precocemente é uma das principais causas de não conformidade com a US SOx, pois deixa tempo insuficiente para avaliar controles essenciais que envolvem tecnologia.
- **Mantenha a independência:** Embora a auditoria interna seja uma das principais partes interessadas na UK SOx, a função não deve ser responsável pela implementação. Em vez disso, a AI deve ajudar a organização com prontidão para a UK SOx por meio de aconselhamento e asseguração.

Dando os próximos passos

- **Torne-a sustentável:** Identifique e valide controles claros e robustos em nível de entidade.
- **Olhe para fora:** Identifique terceiros cujas atividades impactam o ICFR e, portanto, podem estar no escopo.
- **Documente:** Gere uma documentação de processo robusta para ciclos de negócios relevantes, com os donos de processos correspondentes. Identifique e avalie os controles relevantes.
- **Crie processos robustos:** Defina e evidencie um processo robusto para monitoramento contínuo e avaliação de final de ano da eficácia do projeto, concluindo sobre a eficiência operacional dos controles relevantes.
- **Encare o fracasso:** Identifique as falhas ou fraquezas de controles significativos que exigiria consideração detalhada e divulgação de ações para correção. Defina a forma mais apropriada de reporte e acompanhamento das ações corretivas.



O papel da auditoria interna

Automação

Entre muitas perguntas difíceis: "Como a auditoria interna aproveita a automação para acompanhar a automação?"

Nossa visão

Pessoas de norte a sul há muito tempo debaterem uma pergunta incômoda: "Quem veio primeiro, o ovo ou a galinha?

A gestão enfrenta um dilema semelhante quando se trata de auditoria interna: “O que vem em primeiro lugar: colocar nossa casa em ordem e então trazer a auditoria interna? Ou trazer a auditoria interna para começar a nos ajudar a por a casa em ordem?

O problema é particularmente agudo quando se trata da adoção de soluções automatizadas como inteligência artificial e robotização. A implantação pode ser complicada; alguns controles podem ser deixados de lado; a segurança pode ser insuficiente – e tudo isso pode impactar significativamente o ROI esperado pela administração para sua jornada de automação e, pior, criar riscos internos e externos.

Se a administração hesita em envolver seu grupo de auditoria interna por medo de resultados negativos, aqui está sua tréplica: "Automação veio para ficar, mas a tecnologia vai certamente continuar evoluindo. Software, hardware, oportunidades e vulnerabilidades representam um alvo em movimento. Como tal, o valor da automação pode não ser obtido em sua plenitude se você não envolver a auditoria interna”.

Uma vez que a equipe de auditoria interna esteja engajada, quais são as prioridades? Comece ajudando a gestão a encontrar um equilíbrio entre o apetite ao risco e o seu nível de exposição. Conecte-se no início do processo, quando decisões estratégicas sobre automação estão sendo feitas pela primeira vez. Idealmente, essa relação poderá incluir elementos consultivos e de asseguração — ajudando a organização a avaliar o ROI e, em seguida, fornecendo serviços de asseguração e sugerindo melhorias para amparar a implantação desta automação.

Simultaneamente, adapte seu plano de trabalho ao novo ambiente. Avalie os riscos destes novos recursos (processos de negócios impactados, formas de trabalho e novas tecnologias disponibilizadas) em todos os principais domínios de risco, como financeiro, operacional, regulatório, tecnológico e estratégico, e depois priorize com base em critérios de impacto e vulnerabilidade.

Em seguida, inspecione sua própria casa. Determine as habilidades necessárias para auditar soluções automatizadas. Você pode treinar para preencher as lacunas? Ou você terá que recrutar novos funcionários ou especialistas externos com as credenciais necessárias?

E finalmente, você precisará lidar com seu próprio dilema: "Como aproveitar a automação para acompanhar a automação?“

Fatos relevantes

O prognóstico parecia fraco para uma grande empresa de tecnologia com um plano ambicioso de revolucionar a saúde por meio da inteligência artificial (IA), depois que seu supercomputador cuspiu "múltiplos exemplos de recomendações de tratamento inseguras e incorretas" para pacientes com câncer.

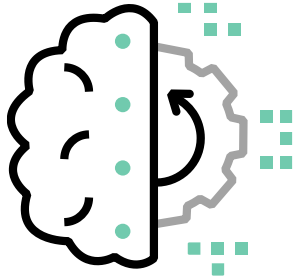
Dados importantes

Em uma pesquisa recente da Deloitte:

83% De executivos disseram que a inteligência artificial vai ser importante para o sucesso de seus negócios nos próximos dois anos.

23% Disseram que sua equipe atualmente audita recursos digitais avançados.

59% Disseram que não estavam envolvidos no desenvolvimento do programa de automação de sua organização.



Para obter mais informações sobre automação

- **Deloitte:** Auditando os riscos de tecnologias disruptivas | Mantenha o ritmo
- **Deloitte:** Movendo a auditoria interna para a era digital: Parte I
- **Deloitte:** Movendo a auditoria interna para a era digital: Parte II

Sinais de alerta

- **Abordagens dispersas e pontuais:** Se o RH está implantando inteligência artificial e o Contas a Pagar está adotando RPA, enquanto o P&D está mexendo com o NLP, você tem uma abordagem fragmentada para a implantação de automação que provavelmente estará repleta de vulnerabilidades.
- **Exclusão da AI:** Se a auditoria interna não tiver um assento na mesa quando as soluções automatizadas estão sendo discutidas pela primeira vez, as chances de implantação bem-sucedida são diminuídas.
- **Falta de acesso:** Um grande obstáculo para a auditoria interna avaliar as soluções automatizadas é a incapacidade de revisar algoritmos e a documentação de desenho das soluções.

Acertando os fundamentos

- **Faça um balanço:** Entenda a estratégia de negócios, a visão pretendida e a jornada relacionada à implantação de soluções automatizadas. Os riscos correspondentes estão adequadamente considerados como parte dessa jornada?
- **Faça perguntas:** Que novos riscos surgem em decorrência dessas novas tecnologias? Como garantir que as métricas e os modelos sejam precisos? Como nos protegemos contra vieses em nossos algoritmos?
- **Assuma o controle:** Esclareça e alinhe os objetivos de negócios para aconselhar de forma mais precisa sobre o desenho das atividades de controle necessárias e/ou realizar revisões pré-implementação.

Dando os próximos passos

- **Estruture:** Crie uma estratégia par apoiar o gerenciamento de riscos de tecnologia e de automação, alinhada à estrutura de governança necessária para endereçar os riscos e atender aos requisitos de conformidade.
- **Pense no todo:** Ao auditar soluções de automação, considere temas como controles, governança, ciclo de vida de desenvolvimento e manutenção, estratégias e revisões de algorítimos.
- **Reformule os seus relatórios:** Modernize seus relatórios para essa nova era. Avalie os tipos de reporte que serão necessários, considerando o modelo mais apropriado para atender aos profissionais de tecnologia e das função de negócios. Determine o enfoque mais apropriado em relação à asseguração *versus* aconselhamento e reconsidere a frequência e a prazos de suas auditorias.

Deloitte.

Anselmo Bonservizzi
Sócio-líder da área de Risk Advisory
abonservizzi@deloitte.com

Camila Boretti
Sócia de Risk Advisory
Accounting & Internal Controls
cboretti@deloitte.com

Paulo Márcio Vitale
Sócio de Risk Advisory
Auditoria Interna
pvitale@deloitte.com

Alex Borges
Sócio de Risk Advisory
Regulatory & Strategic Risks
alborges@deloitte.com

Heloísa Santos
Sócia de Risk Advisory
hesantos@deloitte.com

Luciano Lourenço
Sócio de Risk Advisory
luclourenco@deloitte.com

Christian Silva
Sócio de Risk Advisory
chrsilva@deloitte.com

Guilherme Lockmann
Sócio de Risk Advisory
glockmann@deloitte.com