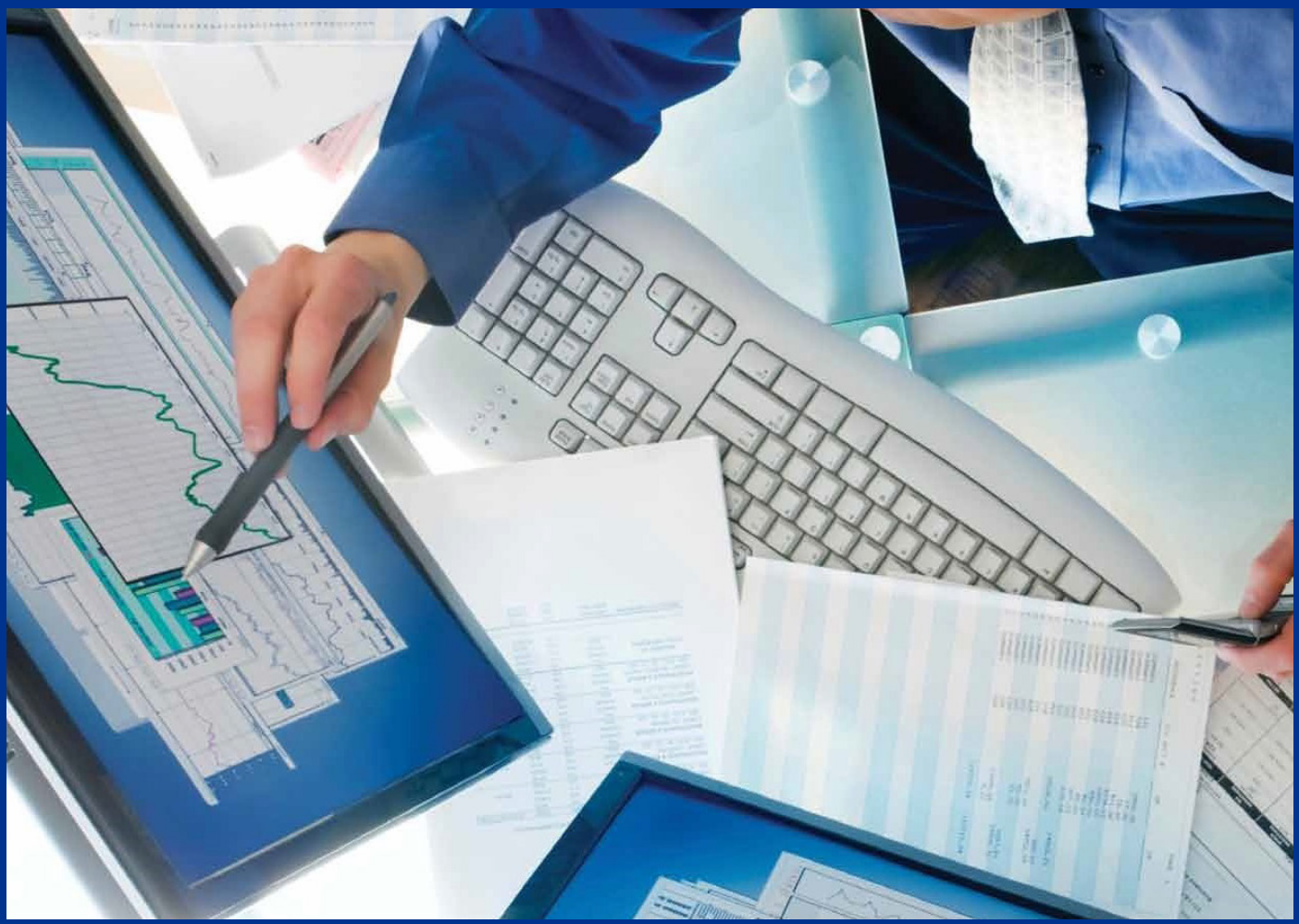
KPMG
cutting through complexity

Padrão de Relatórios de Asseguração

Com base nas Normas ISAE Nº 3402 (NBC TO Nº 3402), ISAE Nº 3000 (NBC TO Nº 3000) e/ou SSAE Nº 18 para Organizações Prestadoras de Serviços



A crescente necessidade de asseguração para as organizações prestadoras de serviços (empresas terceirizadas)

Cada vez mais, as empresas optam por terceirizar funções não essenciais. Porém, cada organização é responsável pelo seu ambiente de controles. Nesse cenário, houve um forte aumento na demanda por asseguração de controles em atividades realizadas por terceiros. Trata-se de uma necessidade impulsionada por fatores como concorrência global, ameaças emergentes e requerimentos regulatórios. A KPMG entende os desafios relacionados à terceirização e ajuda as empresas a suprirem essa crescente demanda por asseguração de controles.

Maior concorrência global

A concorrência econômica global e as pressões de custo fizeram com que as empresas aumentassem a terceirização para prestadoras de serviços. E não estamos falando apenas das tarefas de *back-office*: agora, a terceirização se estende à iniciação, ao registro, ao processamento e aos relatórios das transações de uma organização, o que pode ter um impacto direto nas demonstrações financeiras e nos principais processos empresariais.

Ameaças emergentes

O aumento na terceirização amplia as preocupações relacionadas a riscos e segurança. Violações das informações dos clientes podem acarretar danos operacionais, financeiros e de imagem a partir de falhas de segurança das prestadoras de serviços. Os consumidores também estão mais atentos às medidas tomadas para proteger as informações – dentre elas, informações pessoais identificáveis (PII) e informações protegidas de saúde (PHI). Os riscos apresentados para as empresas aumentam quando as organizações prestadoras de serviços processam e armazenam dados privados e/ou confidenciais dos clientes, realizam o processamento de transações para múltiplos clientes e são auditadas por seus clientes ou por agentes reguladores. Uma análise independente das operações críticas empresariais e de TI que tenham sido terceirizadas pode ajudar as empresas a identificar e controlar esses riscos.

Requerimentos regulatórios

Novos requerimentos regulatórios pressionam as organizações para que estas obtenham e ofereçam asseguração de que os seus controles são eficazes. Os requerimentos contemplam:

- Lei Sarbanes-Oxley (SOX).
- Diretrizes da Superintendência de Instituições Financeiras, incluindo B-10.
- erceirização das atividades, áreas e processos empresariais para o setor de serviços financeiros.
- Leis federais, como a Lei Geral de Proteção de Dados (LGPD).
- Informações de saúde relacionadas às regulamentações de privacidade.

Adicionalmente, os órgãos governamentais tornaram mais rigorosa a aplicação das leis voltadas ao cumprimento dessas regulamentações.

Em relação a maior concorrência global, a resposta consiste em garantir o cumprimento de normas regulatórias, o que também exige a asseguração de que os sistemas e os processos de TI tenham os controles corretos.

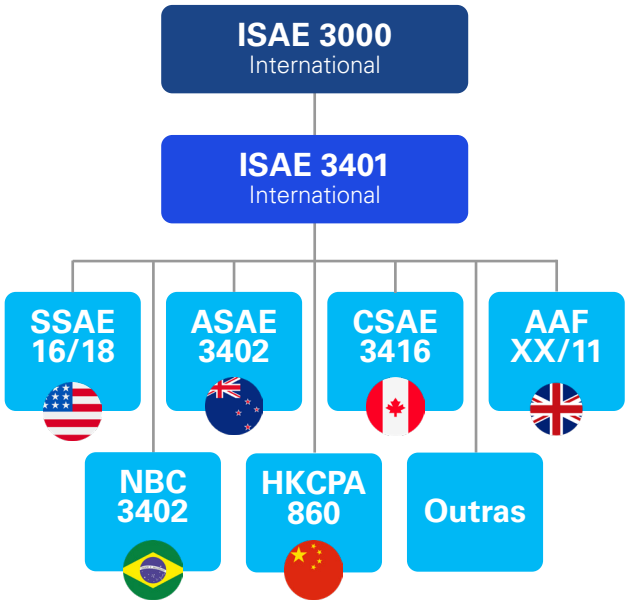
A KPMG pode auxiliar com as suas necessidades de Asseguração/Atestação

A KPMG oferece serviços de asseguração e atestação para auxiliar as organizações a atenderem os requisitos de terceiros no que tange ao exame independente de seus ambientes, sistemas e processos de TI. Os serviços de asseguração mais comuns incluem os relatórios Service Organization Controls (SOC 1 e 2). A KPMG também oferece serviços de propósito especial, tais como os serviços de Procedimentos Pré-Acordados (AUP), para assistir as organizações na emissão de seus relatórios de cumprimento de requisitos de leis, regulamentações ou contratos especificados.

Relatórios de Controle da Organização de Serviço (SOC)

Visão geral

Em 2009, o Conselho Internacional de Normas de Auditoria e Asseguração (IAASB) emitiu a Norma Internacional Sobre Trabalhos de Asseguração (ISAE) 3402, que se tornou uma norma internacionalmente reconhecida para asseguração de organizações prestadoras de serviços. Nos Estados Unidos, o Instituto Americano de Contadores Públicos Certificados (AICPA) emitiu Manifestações sobre a Norma para Trabalhos de Asseguração (SSAE) 18, relatando sobre Controles em uma Organização Prestadora de Serviços. No Brasil, o Conselho Federal de Contabilidade (CFC) emitiu a Norma Brasileira de Contabilidade (NBC-TO) 3402.



Um relatório ISAE 3402/NBC-TO 3402/ SSAE 18, SOC 1 tem o propósito de prestar assistência aos clientes das organizações prestadoras de serviços e aos auditores destas na auditoria de demonstrações financeiras e sobre serviços. Essas informações podem ser relevantes para os Controles Internos sobre a Preparação e a Divulgação de Informações Financeiras (ICOFR) das entidades usuárias. Dado que os relatórios ISAE 3402/NBC TO 3402/SSAE 18, SOC 1 não têm o propósito de cobrir controles não relacionados à emissão de relatórios financeiros, o AICPA incorporou aos relatórios as opções SOC 2 e SOC 3. Esses relatórios foram definidos para auxiliar as organizações prestadoras de serviços a atenderem um conjunto mais amplo de necessidades específicas dos usuários (por exemplo, preocupações acerca de segurança, privacidade, confidencialidade, integridade e disponibilidade).

O relatório SOC é uma representação amplamente reconhecida de que a organização prestadora de serviços passou por uma avaliação rigorosa e independente dos seus controles internos.

Relatório ISAE 3402/NBC TO 3402/SSAE 18 - SOC 1

As normas acima oferecem orientações que possibilitam a um auditor independente (auditor de serviços) utilizar esses relatórios durante seus procedimentos de auditoria das demonstrações financeiras das organizações usuárias, incluindo o planejamento e a opinião sobre os testes de desenho, implementação e eficácia operacional dos seus controles, por meio de um Relatório de Asseguração Razoável. Exige-se que as empresas definam seus próprios objetivos de controle e as atividades que atendem às necessidades dos seus clientes. Um relatório SOC 1 normalmente cobre controles gerais de TI (por exemplo: segurança física e lógica, monitoramento de rede e de sistemas, gerenciamento de incidentes e problemas, desenvolvimento de sistemas e de controle

de mudanças, entre outros), bem como o processamento, a aplicação e outros controles específicos de serviços da transação.

Existem dois tipos de relatórios SOC 1: O Tipo 1 e o Tipo 2. Ambos incluem a descrição do ambiente empresarial e de controles como um todo, dos objetivos dos controles e dos procedimentos de suporte aos controles em funcionamento para que os objetivos sejam alcançados. O relatório Tipo 1 inclui testes quanto ao desenho e à implementação do controle em um data-base específica. Já o relatório Tipo 2 inclui testes detalhados, que o auditor de serviço realiza com os controles da organização prestadora de serviços por um período que geralmente varia de seis a 12 meses. O relatório inicial deve cobrir um período de pelo menos seis meses, exceto se houver circunstâncias que exijam um relatório específico para um período menor – por exemplo, nos casos em que uma organização prestadora de serviços, um sistema ou um aplicativo tenham operado por menos de seis meses.

Os relatórios SOC 1 requerem que a organização prestadora de serviços defina os objetivos de controle que poderão ser relevantes para o Controle Interno sobre a Preparação e Divulgação de Informações Financeiras (ICOFR) das entidades usuárias.

Relatórios SOC 2 e SOC 3

Os relatórios SOC 2 e SOC 3 utilizam os princípios e critérios de serviços, um conjunto de requisitos específicos desenvolvidos pelo AICPA para oferecer asseguração. Os princípios e critérios são definidos visando segurança, disponibilidade, confidencialidade, integridade do processamento e privacidade. Isso foi feito de uma maneira modular, de tal forma que os relatórios SOC 2 ou o SOC 3 cubram um ou mais de um dos princípios, conforme as necessidades da organização prestadora de serviços e de seus usuários, sendo o de segurança o único princípio obrigatório.

Ainda que muitas dessas empresas possam ter concluído no passado os exames SOC 1, cobrindo um assunto que oferece mais valor para os clientes do que o mero Controle Interno sobre a Preparação e Divulgação de Informações Financeiras (ICOFR), elas ainda podem considerar a emissão dos relatórios SOC 2 ou SOC 3 para outros serviços. Por exemplo: pesquisas setoriais indicam que a segurança e a disponibilidade são as principais preocupações quando se considera a adoção da nuvem. Os relatórios SOC 2 e SOC 3 oferecem mecanismos robustos para oferecer a asseguração de terceiros nessas áreas.

O relatório SOC 3 é utilizado para comunicar um nível de asseguração a uma ampla base de usuários sem que seja necessário revelar resultados detalhados de controles e testes. Um relatório SOC 3 pode ser publicamente compartilhado por meio do site da prestadora de serviços. Algumas organizações podem fazer um exame combinado de relatórios SOC 2 e SOC 3 com relatórios customizados para diferentes grupos apoiadores.

Diagnósticos prévios às asseguraçõe

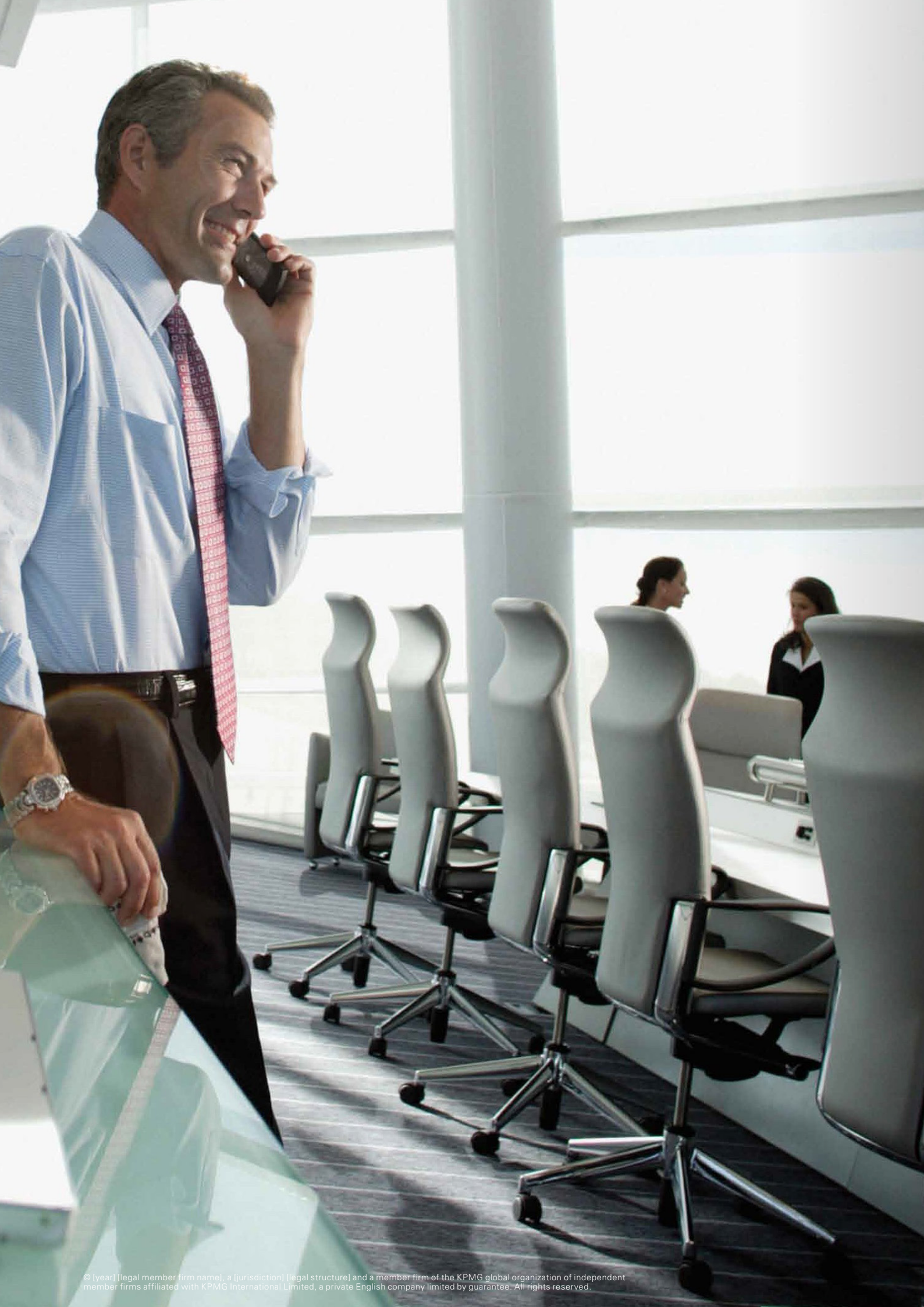
Preocupações sobre o processo do relatório SOC levam algumas organizações prestadoras de serviços a buscar auxílio na avaliação dos seus procedimentos antes de passarem realmente por um exame SOC. Uma avaliação "pré-SOC" ou um diagnóstico ajudam a identificar, nas áreas que serão cobertas em breve por um exame SOC, eventuais deficiências de controle. Estas podem ser corrigidas antes que o período de preparação e divulgação de informações comece. A KPMG tem ampla experiência em apoiar empresas em diagnósticos, seja em serviços tradicionais – tais como hospedagem de aplicativos (Software as a Service), datacenters gerenciados, administração de recurso, processamento de agência de transferência –, ou em serviços novos e emergentes como a computação em nuvem.

A expertise da KPMG em diferentes segmentos permite concluir que a maioria das empresas aprende muito durante o processo de avaliação sobre o seu ambiente de controle e sobre as melhorias necessárias.

Em geral, a avaliação do cenário atual é o primeiro passo; em seguida, são feitas a identificação dos pontos de melhoria e a remediação de eventuais deficiências de controles. Depois que as mudanças adequadas forem efetuadas, se os controles funcionarem por tempo suficiente (aplicável para a asseguração dos relatórios SOC 1 e SOC 2, Tipo 2, somente), o exame real pode começar.

Procedimentos pré-acordados

Procedimentos pré-acordados (AUP) são planejados para que satisfaçam as necessidades de informações das partes que concordaram que a KPMG efetuasse os procedimentos predefinidos. Os procedimentos pré-acordados (AUP) têm boa relação custo-benefício para se avaliar a eficácia dos controles internos, incluindo o cumprimento de regulamentações, políticas e procedimentos, bem como do equilíbrio específico ou da avaliação da conta.



Os serviços de Atestação de Controles da KPMG são adaptados ao seu negócio

Principais fatores para o sucesso da prática de Asseguração da KPMG:

Ela é líder na realização de serviços de Asseguração de Controles. A KPMG tem vasta experiência na prestação de serviços de relatórios SOC e outros serviços de asseguração de controles. Nós construímos relacionamentos de longo prazo com os clientes e nos empenhamos em desenvolvê-los e mantê-los.

Entendemos o negócio da sua empresa. Os profissionais da KPMG detêm profundo conhecimento e experiência em inúmeros processos empresariais dos setores bancário, de energia, de saúde, de seguros, de logística, de serviços de TI e vários outros.

Uma abordagem bem estabelecida. A KPMG desenvolveu metodologias e abordagens criteriosas para a realização de serviços de asseguração de controles. Os profissionais }da área passam por um processo padrão de acreditação.

Metodologia líder

A KPMG lidera o desenvolvimento de padrões de segurança e de controle de TI por meio do seu envolvimento na International Organization for Standardization (ISO), no American Institute of Certified Public Accountants (AICPA), na Information Systems Audit and Control Association (ISACA) e outras instituições.

Desenvolvemos um repositório de objetivos e atividades de controle para orientar a sua empresa por meio do processo de identificação dos objetivos e das atividades de controle, para satisfazer as expectativas dos seus clientes e dos agentes reguladores.

Nossa abordagem utiliza o recurso das normas regulatórias da sua organização em conjunto com os requisitos do serviço de asseguração de controles (por exemplo, o SOC 1) para auxiliar a sua empresa a evitar um ciclo sem fim de mapeamento entre aquelas normas.

Além dos relatórios, a KPMG oferece observações e recomendações para a melhoria do ambiente de controles da sua organização. Essas recomendações são adaptadas ao seu negócio e levam em consideração as normas e as melhores práticas setoriais e regulatórias significativas.

Nossas ferramentas de gerenciamento de projetos

A KPMG desenvolveu ferramentas e técnicas de gerenciamento de projetos que permitem às suas equipes de atendimento aumentar a eficiência por todo o processo do trabalho. A nossa ferramenta de fluxo de trabalho eletrônico permite um melhor gerenciamento de projeto do trabalho, com compartilhamento de informações, comunicações e colaboração entre todos os membros do time em tempo real.

A KPMG trabalha lado a lado com a sua empresa para planejar todas as atividades de asseguração e reduzir as interrupções das operações normais do negócio. Nós envolvemos as principais partes interessadas no início do projeto para promover um entendimento claro dos processos de auditoria e dos objetivos desta. A situação do projeto (project status), suas questões e seus resultados são comunicados ao longo de todo o trabalho.

A abordagem geral da KPMG para os projetos de Asseguração segue três etapas principais: planejamento, trabalho de campo e relatórios. O diagrama a seguir retrata as etapas, as atividades e os produtos do trabalho.

01. Planejamento

- Definir os aplicativos em escopo, infraestrutura e os objetivos de controle;
- Definir o período em escopo daasseguração, bem como o cronograma de trabalho;
- Obtenção da "Descrição da Organização Prestadora de Serviços" descrevendo o seu ambiente e atividades de controle, incluindo aqueles em escopo.

02. Trabalho de campo

- Mapeamento dos riscos de cada processo relacionados aos objetivos de controle definidos no planejamento;
- Identificação e entendimento dos controles relacionados com os riscos mapeados;
- Execução dos procedimentos de teste para avaliação do desenho & implementação dos controles, bem como de sua eficácia operacional (quando aplicável);
- Comunicação de eventuais deficiências.

03. Emissão de relatórios

- Emissão da minuta do relatório para apresentação e discussão com a administração;
- Obtenção da Carta de Representação, confirmando a conclusão dos procedimentos de trabalho;
- Emissão do relatório de Asseguração conforme modelos da Norma aplicável.

Qual relatório é adequado para a sua empresa?

*Nota: Caso a(s) sua(s) resposta(s) à(s) pergunta(s) na primeira coluna seja(m) "sim", então o relatório localizado a direita talvez seja o mais adequado.

	SOC 1	SOC 2	SOC 3
Propósito	Relatório de asseguração razoável com uma opinião sobre controles relacionados às demonstrações financeiras	Relatório de asseguração razoável com uma opinião sobre controles internos relacionados aos seguintes temas: segurança, confidencialidade, disponibilidade, integridade e privacidade	Relatório resumido com os resultados do SOC 2, de modo que possa ser divulgado ao público
Escopo	Controles de como a organização processa, protege e administra informações relevantes para as demonstrações financeiras de seus clientes	Controles de acordo com o „*Trust Service Principles*" (TSP): segurança (obrigatório); confidencialidade, disponibilidade, integridade e privacidade (opcionais)	Controles de acordo com os mesmos princípios selecionados para escopo do SOC 2
Aplicação	Empresas prestadoras de serviço que executam/operacionalizam controles relevantes para as demonstrações financeiras de seus clientes (exemplos: *datacenters*, *softwares*, processadoras de folha de pagamento etc.)	Empresas que administram e gerenciam informações de clientes e desejam demonstrar seus níveis de controles internos relacionados aos seguintes temas: segurança, confidencialidade, disponibilidade, integridade e privacidade	Empresas que desejam divulgar ao público seus princípios e controles relacionados à proteção de dados
Audiência	Clientes da organização prestadora dos serviços e auditores destes clientes	Clientes, parceiros de negócio, investidores e outros *stakeholders*	Público em geral
Benefícios	Avalia se a empresa prestadora de serviços dispõe de controles internos e se estes operam de modo eficaz, permitindo que seus clientes e auditores utilizem esse relatório padronizado em seus processos de auditoria. Sua aplicação é ampla e é aceito mundialmente	Avalia se a empresa prestadora de serviços tem controles internos e se estes operam de modo eficaz, demonstrando aos seus clientes o compliance em relação aos princípios da norma	Diferencial de marketing para novos clientes e targets, demonstrando que a empresa se preocupa com o compliance em seus controles internos

Conclusão

O aumento da concorrência global e das pressões de custos levaram as empresas a optar pela terceirização da maior parte das áreas de negócios para organizações prestadoras de serviços. As preocupações emergentes de segurança e os requerimentos regulatórios somaram-se a esse cenário, enfatizando a exigência por asseguração de controles. A KPMG entende os riscos e os desafios relacionados à terceirização e pode ajudar as empresas a suprir suas necessidades } de asseguração de controles.

A KPMG é líder em serviços de asseguração e atestação e oferece uma gama de serviços adaptada ao seu negócio por meio de uma abordagem criteriosamente construída.

Entre em contato conosco

Para mais informações sobre como a KPMG pode ajudar a sua empresa a gerenciar a asseguração ou atestação de controles e os requisitos de emissão de relatórios, entre em contato.

First name Surname
Additional information
T +49 12 3456-7890
email@kpmg.com

First name Surname
Additional information
T +49 12 3456-7890
email@kpmg.com

First name Surname
Additional information
T +49 12 3456-7890
email@kpmg.com

First name Surname
Additional information
T +49 12 3456-7890
email@kpmg.com

First name Surname
Additional information
T +49 12 3456-7890
email@kpmg.com

First name Surname
Additional information
T +49 12 3456-7890
email@kpmg.com

www.kpmg.com.br

home.kpmg/socialmedia