Auditoria de TI – Processo

Planejamento da auditoria

O planejamento da auditoria engloba todas as atividades necessárias para assegurar que uma auditoria específica realizada pelos auditores possa ser executada de forma completa e eficiente para satisfazer os objetivos da auditoria da organização.

De forma que a auditoria atinja seu objetivo, é necessário que sejam definidos data de início e fim, sejam alocados pessoal adequado e recursos suficientes, de forma a produzir resultados tangíveis na forma de documentação, descobertas, e recomendações.

Uma vez determinado o objetivo da auditoria, assim como a sua prioridade, o planejamento enfatiza as atividades preparatórias de forma que facilite a consecução dos seus objetivos e garanta que a equipe de auditoria terá tudo o que precisa para começar a executar a auditoria.

O planejamento de auditoria também se preocupa com orientações gerais e insumos sobre seu escopo, necessidades de recursos, prazos, protocolos e informações de apoio a serem consideradas e determina necessidades explícitas, prazos, critérios de auditoria e de prova bem como os requisitos processuais.

Durante o planejamento de auditoria, as organizações também definim as expectativas sobre os relatórios de auditoria a serem produzidos ou outros produtos deste trabalho, que serão entregues ao final da auditoria.

Preparação da auditoria

As organizações com programas de auditoria estabelecidas, avaliam sua missão e processos de negócios, sua capacidade operacional e seus ativos de TI para desenvolver suas ações de auditoria, abrangendo todos os aspectos da organização potencialmente sujeitos a auditoria, fazendo uso dos tipos ou abordagens de auditoria mais aplicáveis .

Cada tipo de auditoria de TI tem diferentes fontes de motivação, resultados esperados e objetivos organizacionais. Estes fatores coletivmente direcionam a defnição do escopo da auditoria.

Como parte do planejamento de auditoria, o pessoal do programa de auditoria referem-se a estratégia de auditoria organizacional e identificam as necessidades específicas de auditoria para explicar em detalhes o que será examinado durante a auditoria e o que a organização espera alcançar através da realização da auditoria.

Com um escopo e conjunto de objetivos claramente definidos, a equipe de auditoria e as pessoas dentro da organização que vão apoiar o processo de auditoria podem se preparar para a execução de auditoria:

- identificando e atribuindo os auditores que atuarão e outros recursos necessários,
- revendo os controles relevantes existentes e as informações que serão usadas durante a auditoria,
- e determinando os procedimentos adequados bem como normas e protocolos a serem seguidos.

Alocação de recursos

Dependendo do escopo e complexidade da auditoria que está sendo realizada, auditorias TI podem fazer uso intensivo de recursos. Organizações atribuem auditores e alocam recursos suficientes para apoiar cada auditoria com base no escopo e tipo de auditoria, na natureza do exame exigido para diferentes ativos, processos ou controles, e o cronograma para a conclusão.

Planos de auditoria devem estabelecer as datas de início e de término pretendidos para uma auditoria, bem como quaisquer etapas intermediárias ou pontos de controle necessários durante o projeto.

Se os resultados da auditoria devem ser entregues até uma data específica para o comitê de auditoria, gestão executiva, ou audiências externas, tais como autoridades reguladoras, em seguida, na atribuição de recursos deve-se priorizar o término da auditoria dentro do tempo disponível para satisfazer os prazos especificados.

Quando operando sob menores restrições de tempo, as organizações podem agendar auditorias ou alocar recursos com base na disponibilidade de auditores com as habilidades necessárias e experiência.

Coleta preliminar de dados

Coleta de evidências é um foco primário da realização de auditorias de TI, mas as organizações podem ajudar a garantir a execução de auditoria tempestiva e eficazmente através da coleta de informação durante a fase de planeamento que os auditores terão de analisar durante a auditoria.

Dependendo do tipo e escopo da auditoria, fontes de informação relevantes tipicamente incluem:

- políticas, procedimentos, normas e diretrizes;
- documentação do aplicativo ou sistema, incluindo manuais operacionais;
- definições de configuração de servidores, dispositivos ou componentes de tecnologia;
- descrições dos controles implementados, incluindo controles de segurança; e
- relatórios de auditoria e planos de ação corretivos de auditorias anteriormente realizadas.

Na medida em que a organização conhece os procedimentos de auditoria e critérios de auditoria específicos a serem aplicados pelos auditores, o planejamento de auditoria pode incluir resumos preliminares de evidências necessárias ou checlists de auditoria.

O pessoal envolvidos com papéis coadjuvantes na auditoria podem usar estas informações para disponíbilizar informações prévias e assegurar que os arranjos logísticos necessários tenham sido feitos tais como provisionamento de instalação ou direitos de acesso ao sistema para os auditores além fornecer informações de pessoal de contato que servirão de apoio aos auditores durante a realização da auditoria.

Procedimentos de auditoria e protocolos

Auditorias por definição diferem de avaliações e outros tipos de revisões mais gerais, no sentido de que comparam as características organizacionais com critérios de auditoria formais. Se especificado em normas publicadas, regras ou regulamentos desenvolvidos internamente, os critérios de auditoria devem ser explicitamente definidos e documentados para que os

auditores possam usá-los como base para a análise de processos, controles, capacidades, ou comportamento organizacional coberta pelo escopo de uma auditoria.

A seleção de critérios de auditoria usados para uma determinada auditoria depende do tipo de auditoria, a sua finalidade ou resultados pretendidos, e o conjunto de temas a serem examinados. Da mesma forma, a escolha dos procedimentos de auditoria e protocolos que os auditores irão utilizar reflete o tipo e a finalidade da auditoria e que está sendo auditado.

A lista a seguir identifica algumas fontes importantes de procedimentos de auditoria para diferentes tipos principais de auditorias. A definição do âmbito e objetivos da auditoria durante o planejamento de auditoria geralmente correlaciona os critérios de auditoria que os auditores irão aplicar aos procedimentos e protocolos aplicáveis.

Tipo de auditoria	Procedimentos e protocolos de auditoria
Auditoria Financeira	● Statements on Auditing Standards (SAS) ● Statement on Standards for Attestation Engagements(SSAE) ● International Standards on Auditing (ISA) ● International Professional Practices Framework (IIPF)
Auditoria operacional	● Standard Audit Program Guides
Auditoria de certificação	● ISO/IEC 17021 ● ISO 19011
Auditoria de Sistemas de Informação	● ISACA IT Audit Framework ● ISO/IEC 27006, 27007 and 27008

Em uma auditoria interna, o pessoal envolvido no programa de auditoria da organização geralmente têm o poder de determinar procedimentos e protocolos que melhor se adaptem aos seus objetivos de auditoria. Em serviços de auditoria externa, as organizações ditam menos os procedimentos de auditoria, embora os procedimentos recomendados ou propostos podem estar entre os critérios da organização para selecionar a auditoria externa.

Algumas das tarefas envolvidas na etapa de planejamento são as seguintes:

- Definição do âmbito e objetivos.
- Análise e compreensão dos procedimentos padrão.
- Avaliação do sistema e controles internos.
- Os procedimentos de auditoria e documentação de provas.
- Análise dos fatos encontrados.
- Formação de opinião sobre os controles.
- Apresentação do relatório e recomendações.

Uma das coisas mais difíceis na definição do plano de auditoria de TI é determinar os objetivos e escopo da auditoria. Como orientação, pode-se tomar em consideração as seguintes variáveis para determinar tal alcance:

- Extensão e escopo da auditoria ocorrendo.
- Duração e natureza da avaliação, auditoria interna e externa.
- Dimensão da instalação e nível de complexidade.
- Nível de centralização e distribuição de sistemas e integração de bancos de dados.
- Existência de procedimentos e normas para o ambiente de desenvolvimento e produção.

Em um ambiente informatizado, os controles podem ser classificados como abaixo, que são verificados pelo auditor:

A. Controles de Gestão
   1. Política de Segurança e Normas

2. Constituição de Comitê Gestor
3. Plano de Continuidade de Negócios
4. Metodologia de Desenvolvimento de Sistemas

B. Controles Operacionais

1. Monitoramento de ativos físicos
2. Garantir os controles ambientais adequados, tais como ar-condicionado (pó, controles de temperatura e umidade), condicionamento de energia (UPS on-line funcionam o tempo todo com backups, ligação à terra)

C. Controles Organizacionais

1. Definição de papéis, responsabilidades e deveres dos departamentos, de usuários e departamento de TI.
2. Definição de papéis, responsabilidades e deveres no âmbito do Departamento de TI - como desenvolvedores, operadores e administradores.

D. Controles de Aplicação

1. Cada um dos sistemas e subsistemas de computador deve ter seu próprio conjunto de controles para entradas, processamento e saídas. Controles de processamento também devem assegurar controles de conformidade legal.
2. Durante a realização da auditoria, cada um dos controles precisa ser estudado quanto a sua existência e adequação.

Execução da auditoria

A execução da auditoria é o estágio no processo de auditoria em que a equipe de auditoria realiza o desenvolvimento do plano de auditoria e faz um exame detalhado dos processos, dos ativos de TI e controles, comparando as evidências recolhidas sobre a organização e a sua capacidade e práticas com os requisitos especificados nos critérios de auditoria, nos protocolos relevantes ou nas normas aplicáveis.

As atividades associadas com a realização de uma auditoria de TI incluem o exame por auditores de toda a documentação e informação contextual disponíveis sobre o objeto da auditoria, a coleta de provas através de observação, entrevistas e testes, e da análise das evidências para identificar pontos fracos, deficiências de controle ou outros problemas.

A natureza das tarefas desta etapa muitas vezes exige que o auditor de esteja fisicamente presente em um ou mais ambientes físicos da organização que esta sendo submetida a auditoria. Trabalhar no local facilita a interação com o pessoal de apoio da organização a auditoria ou responsáveis por fornecer informações aos auditores e permitir acesso direto à observação dos ativos de TI e dos controles associados que estão sendo examinados no âmbito da auditoria.

Durante a parte do processo de execução da auditoria, a equipe de auditoria e o pessoal da organizacão auditada envolvidos na auditoria reúnem-se para realizar o *kick-off* da auditoria, definir as expectativas sobre o que e quando será examinado e explicar os métodos de auditoria a serem usados com as informações e as fontes de provas relevantes.

A execução da auditoria compreende a coleta e a análise de evidências, podendo ser preciso que os auditores realizem essas tarefas várias vezes, para garantir que provas suficientes foram analisadas para fundamentar as conclusões da auditoria.

Coleta de provas

Os auditores contam com evidências recolhidas na organização para determinar a medida em que estes elementos examinados na auditoria satisfazem os critérios especificados.

As normas de auditoria fazem distinção entre a ***informação*** fornecida por uma organização ou reunida pelos auditores e ***evidências***. Este último é constituído por informações que os auditores são capazes de verificar através de métodos apropriados para o escopo, objetivos e critérios de auditoria e para o tipo de informações sujeitas a exame.

Nas auditorias de TI, principais atividades de coleta de provas normalmente incluem:

- revisão de documentação fornecida pela organização ou recolhidas a partir de entrevistas com o pessoal,
- observação de procedimentos ou atividades operacionais,
- teste de controles,
- e verificação de configuração técnica de componentes de TI.

Fontes de ***informação***, portanto, tornam-se fontes de ***evidências*** quando, e se, os auditores são capazes de avaliar completamente as informações, confirmar a sua precisão e integridade, e correlacioná-la aos critérios auditados.

Evidências recolhidas pelos auditores fornecem a base para os resultados da auditoria, incluindo as indicações de controles ou determinações de conformidade insuficientes ou ineficazes.

Auditores registram os tipos de informação que examinam e os métodos que utilizam para recolher provas que, em separado dos resultados obtidos das evidencias coletadas e análises realizadas pela auditoria, documentam os passos que cada auditor segue. Descrevendo o processo de auditoria em detalhe, desta forma, ajuda a garantir a confiabilidade e a validade dos resultados da auditoria, permitindo avaliação do trabalho de cada auditor pelo gerente de auditoria ou outros auditores na equipe.

Fontes relevantes de evidências de auditoria de TI variam entre os diferentes tipos de auditorias e seus propósitos e objetivos. Para examinar completamente um processo, sistema ou ambiente que implementa controles administrativos, técnicos e físicos, os auditores geralmente precisam considerar uma ampla gama de critérios correspondentes a muitas fontes de informação e métodos de avaliação.

As diretrizes de auditoria apresentados na ISO 19011 identificam muitas fontes de informação que auditores podem selecionar dependendo do escopo de auditoria, a complexidade e os critérios que devem ser atendidos, incluindo:

- documentos, tais como políticas, planos, procedimentos, normas, orientações, especificações técnicas, contratos, licenças e acordos de nível de serviço;
- entrevistas com o pessoal da organização responsável pela exploração ou gestão o tema em análise;
- observação direta de atividades que ocorrem no ambiente organizacional;
- aplicações, bancos de dados, interfaces de usuário e outros componentes técnicos;
- Os dados de desempenho, tais como classificações de satisfação de clientes e fornecedores ou qualidade relatórios produzidos por terceiros;
- e testes de controle simulados ou reais, modelagem ou exercícios.

Ao realizar auditorias de organizações ou assunto grandes ou complexos, o volume de informação de auditorias deve ser considerado no processo de coleta de provas pois pode

exceder a capacidade da equipe de auditoria. Em tais casos, os auditores podem envolver-se em amostragem de informações, aplicando métodos de auditoria a um subconjunto das informações disponíveis, e utilizando os resultados para realizar a análise e desenvolver as conclusões da auditoria. O uso de amostragem pode melhorar a viabilidade e a relação custo-benefíio de uma auditoria, mas impõe requisitos processuais adicionais aos auditores para certificar-se de que os métodos de amostragem utilizados em uma auditoria são sólidos, apropriados para o tipo de auditoria, e estatisticamente válidos e que a amostra retirada é verdadeiramente representativa de todo o conjunto de informações.

Análise de evidências

O objetivo principal de obtenção de evidências é permitir que os auditores correlacionem as evidências aos critérios de auditoria aplicáveis e analisem as evidências para determinar a extensão em que esses critérios estão preenchidos. Técnicas para analisar as evidências de auditoria abrangem uma ampla gama de métodos; auditores selecionam os métodos mais apropriados com base no tipo de controle a ser analisado e do tipo de auditoria e seu propósito e objetivos.

Orientações disponíveis na análise de provas recomendam métodos diferentes, utilizados isoladamente ou em combinação, para avaliar os controles administrativos, técnicos e físicos.

A tabela a seguir lista os métodos representativos e as fontes de evidências a que se aplicam.

Aplicabilidade dos métodos de auditoria para diferentes tipos de provas

Métodos	Aplicabilidade
Exame/Verificação	● Documentação de sistema, especificações, diagramas ●Planos, políticas, procedimentos, instruções, diretrizes ● Normas, frameworks, metodologias
Entrevista	● Funcionários com responsabilidade operacional para assuntos de auditoria ● Os gerentes responsáveis pela governança, risco e conformidade ● Os clientes, pessoal de apoio, os usuários finais do sistema
Observação	● Funcionalidade de software ou de hardware ● Atividades operacionais, processos, práticas, exercícios ● Comportamento pessoal
Teste	● Componentes de tecnologia ● Dispositivos de Hardware ● Aplicações de software e sistemas ● Procedimentos de controle e capacidades técnicas

A escolha dos métodos de auditoria também leva em conta a quantidade e qualidade da interação entre o auditor e pessoal na organização que está sendo auditada, o nível de acesso que o auditor tem de componentes de TI ou outros objetos de auditoria, e a localização do auditor (por exemplo, no local ou fora do local) durante o exame .

Métodos analíticos também podem ser executados em diferentes níveis de rigor. Objetivos e requisitos relativos à utilização dos resultados da auditoria direcionam a abrangência das atividades de análise ou teste.

Os auditores são responsáveis por descrever os procedimentos analíticos específicos que eles usam em seus registros ou outros documentos que ficam disponveis aos gestores da auditoria e aos executivos da organização para ajudar a comprovar a qualidade da auditoria.

Critérios utilizados na área de auditoria de TI normalmente incluem requisitos que podem ser determinados objetivamente, bem como aqueles que envolvem o julgamento dos auditores que recolhem e analisam as evidências. Auditores consideram tanto o tipo de evidência e sua fonte para julgar a sua confiabilidade e suficiência para apoiar os resultados gerados pela auditoria.

As auditorias de TI muitas vezes incluem características técnicas, tais como um sistema, configuração de dispositivos e implementação de controles, que podem ser confirmados através de métodos de teste automatizados.

Examinar esses elementos exige que os auditores tenham conhecimento suficiente dos procedimentos de teste aplicáveis e as ferramentas envolvidas, mas a interpretação dos resultados geralmente implica uma comparação objetiva entre os resultados do teste e critérios de auditoria.

Em contraste, os auditores revisando documentação ou analisando de informações obtidas através de entrevistas ou observação precisa exercitar o julgamento para avaliar as evidencias de forma consistente com os padrões de prática profissional e com objetividade, competência e devido cuidado.

Relato dos Resultados

Os resultados da auditoria resultam da comparação das evidências aos critérios de auditoria. Dependendo do tipo de auditoria e seus objetivos, os relatos podem endereçar todos os critérios ou apenas os elementos que auditores julgarema ser deficientes ou insuficientemente apoiadas por evidências. Quase todas as metodologias de auditoria enfatizam a importância de apresentar as constatações de deficiências ou não conformidades ao critérios auditados, uma vez que estas áreas representam as fontes de risco que a organização auditada precisa responder.

Dependendo dos objetivos da auditoria e o público-alvo para o relatório de auditoria, o conteúdo do relatório pode incluir constatações satisfatórias e áreas de conformidade, bem como as deficiências ou falhas.

O formato e o conteúdo específico exigido em um relatório de auditoria, o qual influencia o nível de detalhe que o relatório inclui, são definidos pelos fins para os quais o relatório será utilizado pelas partes interessadas (internas e externas) com as quais serão compartilhados.

Como primeiro requisito de um trabalho de auditoria, o relatório de auditoria deve fornecer informações suficientes para ser considerardo como um produto decorrente de uma investigação. Detalhes completos sobre o processo de auditoria devem ser capturados dos registros de auditoria, que fornecem uma prestação de contas das evidências que cada auditor considerou, os critérios que aplicou, e os métodos de auditoria utilizados. O nível de detalhe refletido nos registros do auditor são raramente incluídos nos relatórios de auditoria, mas esta documentação de apoio pode ser referenciada a partir do relatório de auditoria, se necessário.

Além de um resumo global da auditoria e seus resultados, um relatório de auditoria geralmente contém informações como:

- finalidade e os objetivos para a realização da auditoria;
- âmbito da auditoria, incluindo elementos organizacionais, funcionais ou técnicas a que a auditoria se aplica;
- identificação do cliente de auditoria;
- identificação dos participantes da auditoria, incluindo auditores e as sujeitas à auditoria;
- período de tempo durante o qual a auditoria teve lugar;
- locais onde ocorreram auditoria, incluindo instalações de organização e locais de trabalho auditor fora da organização, se houver;

- critérios especificados para a auditoria;
- constatações de auditoria e provas;
- as conclusões da auditoria, incluindo as recomendações do auditor; e
- resultados de auditorias, potencialmente incluindo sucesso ou fracasso ou determinação da medida em que a organização satisfaz os critérios de auditoria.

A maioria das metodologias e orientações de auditoria distinguem entre ***constatações*** da auditoria e ***conclusões*** da auditoria.

Constatações correspondem diretamente aos critérios de auditoria e indicam, ou não, se o objeto auditado satisfaz cada critério de auditoria, enquanto que ***conclusões*** são evidências e opiniões baseadas na experiência dos auditores sobre as implicações das constatações para a organização. Conclusões podem incluir inferências sobre o porquê de diferentes ***constatações*** ocorreram, recomendações para a mitigação de risco ou remediar irregularidades mencionadas nas constatações, se os objetivos da auditoria foram alcançados, ou a eficácia das capacidades organizacionais em exame.

Objetivos organizacionais para auditorias de TI nem sempre incluem ações corretivas ou identificação de oportunidades de melhoria operacional, especialmente se uma determinação de "sucesso" para a organização não exigem uma resposta às constatações da auditoria.

As normas de auditoria prevalentes e orientações para os auditores internos enfatizam a importância não apenas de fazer recomendações sobre medidas correctivas para resolver constatações da auditoria, mas também para verificar que as ações corretivas sejam tomadas.

Muitos tipos de auditorias externas incluem recomendações sobre medidas corretivas e respostas do corpo gerencial da organização auditada, como concordância ou discordância com as recomendações e compromissos para implementar planos de ação para remediar fraquezas.

Os resultados da auditoria descrevem em detalhe os pontos fracos de controle, deficiências operacionais, e outras fontes de risco para uma organização. Os relatórios de auditoria geralmente incluem informações sensíveis ou confidenciais que a organização não quer que seja tornada pública ou divulgada aos concorrentes, clientes, parceiros de negócios, ou para os reguladores ou autoridades de supervisão, a menos que tal divulgação seja explicitamente necessária. As organizações precisam garantir que os relatórios de auditoria e papéis de trabalho detalhando as descobertas do auditor tenham o acesso controlado de forma rigorosa para limitar a divulgação apenas para pessoas autorizadas e com uma necessidade legítima de ter a informação.

Usando as informações nos relatórios de auditoria

Na conclusão do processo de auditoria, os auditores finalizam o relatório de auditoria e entrega a organização auditada. Principais destinatários dos relatórios de auditoria produzidos em ambas as auditorias internas e externas incluem a comissão de auditoria e gestão executiva da organização auditada. Os resultados das auditorias externas devem ser normalmente comunicados a terceiros autorizados, tais como reguladores, mas a informação distribuída fora da organização pode não incluir o relatório de auditoria inteira.

Um objetivo chave para auditorias externas é atingir um resultado bem sucedido, onde o sucesso pode significar uma auditoria que aborda todos os elementos definidos no seu âmbito, que produz poucos ou nenhum significativas descobertas que justifique uma ação corretiva, ou que melhora nas constatações de auditoria anteriores em termos de número ou o significado

das constatações e recomendações. Organizações auditadas que endossam sua eficácia operacional, processos de negócios, ou controles internos pode divulgar os resultados globais ou, no caso de empresas de capital aberto, resumir os resultados em documentos oficiais.

Os relatórios de auditoria das auditorias internas também podem ser fornecidos aos reguladores ou auditores externos como evidência para apoiar as auditorias externas. Além de entregar os resultados da auditoria às partes interessadas externas para suportar os requisitos de conformidade e de supervisão, organizações usam a informação em relatórios de auditoria interna para fazer melhorias na eficácia das suas capacidades operacionais e corrigirem falhas ou áreas de não-conformidade.

Falhas de controle da organização, deficiência ou áreas de não conformidade identificados em constatações de auditoria apresentam algum nível de risco. As organizações precisam entender a gravidade do impacto que poderia ocorrer ou a magnitude ou risco associado a cada descoberta para determinar a resposta mais adequada. Em alguns tipos de auditoria de TI, auditores fornecem uma estimativa de risco ou atribuem níveis relativos (por exemplo, alta, moderada, baixa) ao risco ou factores determinantes como a probabilidade e impacto. Precisar e caracteriz o risco para uma determinada organização, no entanto, normalmente requer conhecimento detalhado dos ativos da organização e objetivos de controle, bem como o seu nível de tolerância a risco ou seja, nível de risco que a organização está disposta a aceitar. Os auditores internos podem, portanto, ser melhor posicionada do que os auditores externos para avaliar o risco de conclusões da auditoria. Ambos os auditores internos e externos, muitas vezes precisam trabalhar em colaboração com os gestores de risco e do pessoal organizacionais responsáveis pelos sistemas auditadas, os ativos de TI e processos de negócios para avaliar com precisão o risco representado pelos resultados de auditoria

Respondendo aos resultados da auditoria

Relatórios de auditoria com constatações e conclusões que justificam uma ação corretiva, monitoramento ou acompanhamento (*follow-up*) pela organização auditada se torna uma importante contribuição para o processo de planejamento e execução de respostas organizacionais adequadas.

O melhor cenário para uma organização passando por auditorias de TI em conjunto com auditorias financeira, de conformidade ou de certificação é que os auditores vão determinar se organização está aderente e em conformidade com os requisitos ou certificação (ou recertificação) dos critérios aplicáveis.

Um princípio fundamental na melhoria contínua, porém, é que há sempre maneiras de executar melhor, para que as organizações envolvidas em esses tipos de auditorias são motivadas pelo menos em parte pela necessidade de identificar oportunidades para melhorar.

Além de aumentar o nível de conformidade com os critérios de auditoria ou as normas e práticas que representam, melhorias organizacionais podem vir de uma variedade de fontes, incluindo potencialmente reengenharia de processos de negócios ou de otimização, ou a introdução de novas tecnologias ou controles processuais para os processos operacionais existentes.

As organizações também podem planejar melhorias nas capacidades ou processos, alinhando suas práticas internas para modelos de maturidade como o *Capability Maturity Model*

Integration (CMMI), onde a adoção e gestão eficaz dos processos e procedimentos padrão corresponde a níveis mais elevados de maturidade.

As constatações de fraquezas no controle ou não conformidades organizacionais representam algum nível de risco para a organização se esta não atuar para resolver os problemas identificados.

As organizações precisam avaliar o risco associado com os achados de auditoria e determinar a melhor resposta a esse risco. Assim como avaliação de risco dentro do contexto mais amplo de gestão de riscos, ajuda as organizações a priorizar suas atividades de auditoria, avaliação de risco de ameaças ou vulnerabilidades associadas com os achados de auditoria suporta a priorização de respostas aos riscos.

O conjunto de respostas possíveis riscos incluem a mitigação, prevenção, transferência, ou aceitação. A transferência de riscos e aceitação não requerem a modificação direta para operações ou controles da organização, mas a mitigação e prevenção ambos exigem mudanças nos controles ou capacidades operacionais executados pelas organizações.

A mitigação reduz ou elimina o risco através da adição ou aperfeiçoamento de controles, enquanto que evitar riscos ou remover funções faz com que a organização deixe de executar atividades excessivamente arriscadas de forma que já não estejam mais na sua esfera de operações.

As organizações precisam acompanhar as suas respostas às constatações da auditoria por meio de monitoramento e atividades de acompanhamento, para garantir que eles cumpram os compromissos documentados nos relatórios finais de auditoria ou planos de correção e para fornecer informações para equipes de auditoria posteriores sobre mudanças implementadas desde a auditoria anterior.

Bibliografia:

The Basics Of IT Audit - Purposes, Processes, And Practical Information, Stephen D. Gantz

Professional Programme – Information Technology And Systems Audit - Module 2 - Paper 4 - ICSI