Auditoria de Sistemas

Prof. Luiz Antonio Ferraro Mathias

Aula 04

Planejamento da Auditoria

Planejamento da Auditoria

Uma atividade de auditoria pode ser dividida em três fases: planejamento, execução (supervisão) e relatório.

Uma fase vital para qualquer contrato de auditoria é o seu **planejamento**. Ele desempenha o mesmo papel que em outras áreas, na vida pessoal, no desenvolvimento de um novo produto, entre outros. Dele resulta um arranjo ordenado dos passos necessários à condução de determinado objetivo. Tudo que é feito de forma organizada está fadado ao sucesso. O planejamento da auditoria envolve vários passos importantes.

Obtenção de conhecimento do negócio e da organização representa a etapa crítica neste processo, pois estabelece a base para a realização de muitos outros procedimentos de auditoria. Ao planejar o seu trabalho, o auditor toma importantes decisões sobre a relevância e risco de auditoria. Um produto importante do planejamento envolve a tomada de decisões preliminares sobre a estratégia a ser seguida.

Após a etapa do planejamento, vem a supervisão. Esta envolve o direcionamento dos trabalhos dos assistentes para atingir os objetivos de auditoria e verificar se os objetivos foram de fato atingidos. A extensão da supervisão necessária em um contrato depende da qualificação das pessoas que realizam os trabalhos, entre outros fatores. Com isto, ao planejar uma auditoria e sua supervisão, também deve ser previsto quantos membros da equipe são inexperientes e quantos são experientes.

Planejamento da Auditoria

A auditoria envolve alguns importantes atores:

a) Auditor: Profissional preparado para auditar. Tem formação, capacitação, certificação profissional, minimamente preparado para fazer uma validação, uma análise de conformidade nos trabalhos de campo;

b) Auditado: Aquele que é avaliado. Aquele cujos controles estão sobre sua responsabilidade e que serão verificados e validados. Aquele colaborador de certo departamento alvo da auditoria;

c) Cliente: Aquele que solicita ou contrata o trabalho de auditoria. Aquele que apoia, patrocina, defende e aprova a contratação. Ex.: Auditoria de SI em uma empresa X. O cliente é o(a) diretor(a) da empresa, visto que foi ele(a) que fez e estabeleceu a contratação, o escopo etc.;

Planejamento da Auditoria

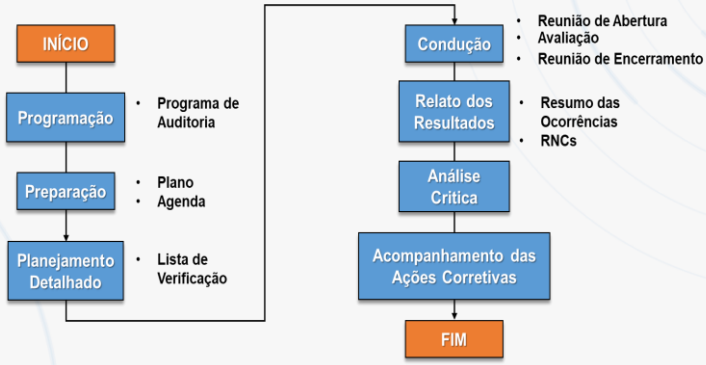
d) Especialista: Alguém que tem especificação em certa área para avaliar e transmitir para a equipe de auditoria. Ele detém conhecimentos técnicos sobre determinada ferramenta em um ambiente computacional, por exemplo. Ele não é auditor, não tem formação de auditoria, mas possui um alto conhecimento em certo ambiente e vai auxiliar durante o processo de auditoria, fazendo uma análise e reportando ao auditor as condições;

e) Guia: Facilitador. Colaborador da empresa que conhece as áreas, os departamentos, os processos e vai facilitar a vida do auditor. Ele tende a contribuir com o trabalho e desempenho do serviço de auditoria, visto ele conhece a empresa;

f) Observador: pode ser alguém da administração pública, autarquia ou órgão regulador que acompanha o serviço de auditoria em execução, bem como um prestador de serviço, um fornecedor de sistema informatizado etc.

Planejamento da Auditoria

Uma auditoria pode ser conduzida através de ciclos, cada qual baseado na execução de fases específica:



Planejamento da Auditoria

As fases da auditoria envolvem um conjunto definido de atividades, assim distribuídas:

i. **Coleta das informações**: envolve contato inicial com o auditado e verificação da amplitude do trabalho no sentido de compreender o tamanho da organização a ser auditada; a complexidade do trabalho a ser realizado; a abrangência das atividades estarão envolvidas e as regras de segurança;

i. **Preparação**: seleção da equipe de acordo com competências e habilidades; definição da duração estimada dos trabalhos; análise de aspectos e requisitos contratuais; verificação do idioma que será empregado na comunicação com a equipe do auditado; reunião com a equipe; elaboração/adequação das listas de verificação (checklist);

Planejamento da Auditoria

iii. **Escolha das datas**: com atenção especial para férias coletivas, férias de pessoas chave dos processos a serem auditados, feriados nacionais e locais, greves, acontecimentos marcantes (congressos, feiras etc.) regionais;

iv. **Notificações e programa de auditoria**: definição dos processos e controles que serão auditados, requisitos de normais legais e de referência (ISO), expor critérios e programa de auditoria, escopo, unidades e processos, datas e lugares, aspectos logísticos e de confidencialidade;

v. **Reunião de abertura dos trabalhos de auditoria**: organizada e conduzida pelo auditor líder, que pode estar sozinho ou com parte da equipe e representantes da empresa a ser auditada, oportunidade em que se confirma o programa da auditoria, canais de comunicação, esclarece dúvidas, confirma normas aplicáveis ao trabalho, esclarece os conceitos de conformidade e não conformidade, e define reuniões regulares;

Planejamento da Auditoria

vi. **Auditoria de campo**: realização do trabalho de validação pela equipe de auditores e especialistas com o objetivo de garantir a abrangência prevista no contrato. Deve haver clareza no apontamento de fatos, situações, não conformidades etc., entrevistas com a equipe do auditado, registros de inspeções, atas e medições;

vii. **Reunião de encerramento do trabalho de campo**: agradecimentos aos participantes, breve resumo dos trabalhos realizados, exposição das não conformidades e oportunidades de melhoria, esclarecimento de dúvidas, discussão de pontos específicos, definição de prazos de saneamento e adequação de não conformidades e medidas de supervisão, se necessário;

viii. **Relatório final**: que deve conter, minimamente - dados da organização, objetivos e escopo da auditoria, grupos e áreas auditadas, metodologia empregada, normas legais e de referência aplicadas, resultados das validações e conclusões;

Planejamento da Auditoria

ix. **Ações corretivas**: fase em que ocorre a investigação, pelo auditado, das não conformidades apontadas no relatório de auditoria, com documentação das ações saneadoras, implementação do plano de ação e medição da efetividade deste;

x. **Acompanhamento pelos auditores**: atividade cuja realização depende do escopo da contratação. Nesta fase, a auditoria obtém respostas para as não conformidades, cumprimento dos prazos, e confirmação da efetividade das ações realizadas.

Conclusões do trabalho de campo

Na fase de conclusão da auditoria, o auditor frequentemente irá trabalhar sob rígidas condições de prazo, pois os clientes querem obter o parecer o mais cedo possível. Nada mais justo, porém é importante lembrar que não se pode sucumbir às pressões decorrentes do trabalho sob pena de emitir um relatório simples demais, de pouca qualidade ou até mesmo com poucos detalhes.

Na conclusão do trabalho de campo, o auditor deve ter certeza de que já fez todas as entrevistas necessárias, coletou todos os dados necessários para analisar as evidências e tecer um parecer correto, que auxilie o cliente a melhorar o seu ambiente de TI aumentando a sua disponibilidade, o seu caráter confidencial e a sua integridade de dados. Uma boa estratégia é revisar as entrevistas com as pessoas envolvidas na administração da informática, relendo-as e confirmando os dados com as pessoas envolvidas para garantir a integridade de tais informações. Também é importante revisar atas de possíveis reuniões passadas, a fim de se fazer a mesma confirmação.

Conclusões do trabalho de campo

As normas de auditorias geralmente aceitas não exigem que vulnerabilidades relevantes sejam identificadas separadamente. Porém é muito interessante, para um maior entendimento e até programação de investimentos por parte do cliente, que as vulnerabilidades sejam divididas em níveis de severidade, acusando suas consequências caso não sejam remediadas e a medida do risco destas, para se prever em que momento tal fraqueza pode ser explorada por uma ameaça.

Ao avaliar o que foi verificado na auditoria, o auditor tem por objetivo determinar o tipo de parecer a ser emitido e determinar se a auditoria seguiu as normas geralmente aceitas. Para formar opinião sobre as demonstrações contábeis, o auditor deve assimilar todas as evidências que constatou durante a auditoria, da mesma forma que o auditor de sistemas informatizados deve reunir todo tipo de informação coletada do ambiente de TI do cliente. O primeiro passo é identificar as distorções que foram encontradas e não foram corrigidas pelo administrador de TI Em casos de pouca severidade, o auditor pode ressaltar o fato de que a alteração pode ser feita mais tarde, porém, em casos graves, ele também pode pedir que a alteração seja feita imediatamente.

Conclusões do trabalho de campo

Na conclusão da auditoria, é necessário que todas as constatações sejam resumidas e avaliadas. Aqui também é constatada a não conformidade com a norma aceita pelo cliente como sendo padrão de segurança de informação.