

Norma 1204 de Auditoria e Garantia de SI Materialidade

A natureza especializada da auditoria e garantia de sistemas de informação (SI) e a capacidade necessária para realizar essas contratações requerem o estabelecimento de normas que se apliquem especificamente à auditoria e garantia de SI. O desenvolvimento e a disseminação das normas de auditoria e garantia de SI são fundamentais como contribuição profissional da ISACA[®] para a comunidade de auditoria.

As normas de auditoria e garantia de SI definem requisitos obrigatórios para auditoria, emissão de relatórios e orientações sobre:

- Profissionais de auditoria e garantia de SI no nível mínimo de desempenho aceitável exigido para cumprir as responsabilidades profissionais estabelecidas no Código de Ética Profissional da ISACA;
- A gerência e outras partes interessadas sobre as expectativas da profissão no que se refere às atividades daqueles que a exercem;
- Os requisitos necessários para os detentores da certificação Certified Information Systems Auditor[®] (CISA[®]) (Auditor Certificado em Sistemas de Informação). A não conformidade com essas normas pode resultar numa investigação da conduta do detentor da CISA pelo Conselho de Administração da ISACA ou pelo comitê apropriado e, finalmente, em ação disciplinar.

Profissionais de auditoria e garantia devem incluir uma declaração em seu trabalho, quando apropriado, de que a contratação foi realizada de acordo com as normas de auditoria e garantia de SI da ISACA ou outras normas profissionais aplicáveis.

A estrutura ITAF[™] para o profissional de auditoria e garantia de SI apresenta diversos níveis de diretrizes:

- **Normas**, divididas em três categorias:
 - Normas gerais (série 1000) - são os princípios norteadores sob os quais funciona a profissão de auditoria e garantia de SI. As normas se aplicam à realização de todas as tarefas, e lidam com a ética, a independência, a objetividade e o devido cuidado, bem como conhecimento, competência e habilidade do profissional de auditoria e garantia de SI. As declarações de normas (em **negrito**) são obrigatórias.
 - Normas de desempenho (série 1200) – tratam da realização da contratação, por exemplo, planejamento e supervisão, definição de escopo, risco e materialidade, mobilização de recursos, gestão de supervisão e tarefa, evidência de auditoria e garantia, e o exercício de julgamento profissional, bem como o devido cuidado.
 - Normas de relatório (série 1400) - abordam os tipos de relatórios, os meios de comunicação e as informações comunicadas
- **Diretrizes**, em apoio às normas, e também divididas em três categorias:
 - Diretrizes gerais (série 2000)
 - Diretrizes de desempenho (série 2200)
 - Diretrizes de relatório (série 2400)
- **Ferramentas e técnicas**, oferecendo orientação adicional para profissionais de auditoria e garantia de SI, por exemplo, documentos, programas de auditoria/garantia de SI, a família de produtos COBIT[®] 5

Um glossário on-line de termos usados na ITAF é fornecido em www.isaca.org/glossary.

Ressalva: A ISACA desenvolveu este guia visando definir o nível mínimo de desempenho aceitável exigido para dar resposta às responsabilidades profissionais estabelecidas no Código de Ética Profissional da ISACA. A ISACA não oferece qualquer garantia de que o uso deste produto irá assegurar um resultado bem-sucedido. A publicação não deve ser considerada parte integrante de quaisquer procedimentos e testes apropriados, ou de outros procedimentos e testes também voltados para a obtenção dos mesmos resultados. Ao determinar a propriedade de qualquer procedimento ou teste específico, profissionais de controle devem aplicar seu próprio juízo profissional às circunstâncias específicas de controle apresentadas por determinados sistemas ou ambientes de SI.

O ISACA Professional Standards and Career Management Committee (Comitê de Normas Profissionais e Gestão de Carreira, PSCMC) está comprometido em realizar uma ampla consulta na preparação de normas e diretrizes. Antes de divulgar qualquer documento, uma versão preliminar é divulgada internacionalmente para ser submetida à avaliação pública. As avaliações também podem ser enviadas aos cuidados do diretor de desenvolvimento de normas profissionais por e-mail (standards@isaca.org), fax (+1.847. 253.1443) ou correio (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

ISACA 2012-2013 Professional Standards and Career Management Committee	
Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaysia
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Norma 1204 de Auditoria e Garantia de SI – Materialidade

Declarações

- 1204.1** Profissionais de auditoria e garantia de SI deverão considerar fatores como fraqueza potencial ou ausência de controles enquanto planeja uma contratação, e se tal fraqueza ou ausência de controles pode resultar em deficiência significativa ou fraqueza material.
- 1204.2** Profissionais de auditoria e garantia de SI devem considerar a materialidade e sua relação com o risco de auditoria ao determinar a natureza, época e extensão dos procedimentos de auditoria.
- 1204.3** Profissionais de auditoria e garantia de SI deverão considerar o efeito cumulativo de deficiências ou fraquezas de controle secundárias, e se a ausência de controles se traduz em deficiência significativa ou fraqueza material.
- 1204.4** Profissionais de auditoria e garantia de SI deverão divulgar os seguintes itens no relatório:
- Ausência de controles ou controles ineficazes
 - Importância das deficiências de controle
 - Probabilidade dessas fraquezas resultarem em uma deficiência significativa ou fraqueza material.
-

Aspectos principais

Na realização de uma contratação, profissionais de auditoria e garantia de SI devem:

- Aplicar o conceito de materialidade em:
 - Planejamento e realização da contratação
 - Avaliação do efeito de itens, processos, controles ou erros específicos
- Qualquer deficiência, fraqueza ou falta de diretrizes, procedimentos e controles apropriados deve ser avaliada nas circunstâncias específicas da contratação.
- Considerar definições de materialidade quando fornecidas por autoridades legislativas ou regulamentadoras.
 - Observar que a avaliação de materialidade e Risco de Auditoria pode variar de tempos em tempos, dependendo das circunstâncias e da alteração do ambiente
 - Tentar reduzir o risco de auditoria a um nível aceitável e atender aos objetivos enquanto planeja e realiza a contratação.
 - Considerar a Materialidade ao determinar a natureza, época e extensão dos procedimentos de auditoria.
 - Reduzir o risco de auditoria para áreas sujeitas a maior materialidade, estendendo o teste de controles (reduzir o risco de controle) e/ou estendendo os procedimentos de testes substantivos (reduzir o risco de detecção).
 - Avaliar o efeito de controles de compensação, e se tais controles são eficazes e determinar se uma deficiência de controle ou combinação de deficiências de controle seja ou não uma fraqueza material.
 - Considerar o efeito cumulativo de vários erros ou falhas de controle ao determinar a materialidade.
 - Considerar não somente a dimensão, mas também a natureza das deficiências de controle e as circunstâncias específicas de sua ocorrência ao avaliar seu efeito geral na opinião ou na conclusão da auditoria.
-

Norma 1204 de Auditoria e Garantia de SI – Materialidade

Termo	Definição
Risco de auditoria	<p>O risco de chegar a uma conclusão incorreta com base em resultados da auditoria. Os três componentes de risco da auditoria são:</p> <ul style="list-style-type: none"> • Risco de controle • Risco de detecção • Risco inerente
Fraqueza material	<p>Uma deficiência ou combinação de deficiências no controle interno, de tal forma que haja uma possibilidade razoável de que uma distorção relevante não seja impedida ou detectada em tempo hábil.</p> <p>A fraqueza no controle é considerada material se a ausência do controle resultar em falha no fornecimento de garantia razoável de que o objetivo de controle será satisfeito. Uma fraqueza classificada como material significa que:</p> <ul style="list-style-type: none"> • Os controles não estão no lugar e/ou os controles não estão em uso e/ou os controles são inadequados • Permite agravamento <p>Há uma relação inversa entre materialidade e nível do risco de auditoria aceitável ao profissional de auditoria ou garantia de SI, ou seja, quanto maior o nível da materialidade, menor a aceitabilidade do risco de auditoria, e vice-versa.</p>
Materialidade	<p>Um conceito de auditoria relacionado à importância de um item de informação com relação a seu impacto ou efeito no funcionamento da entidade que está sendo auditada. Uma expressão da significância ou importância relativa de um tema específico no contexto da empresa, como um todo.</p>

Vinculação a normas e diretrizes

Tipo	Título
Norma	1201 - Planejamento de contratação
Norma	1202 - Avaliação de Risco no Planejamento
Norma	1207 - Irregularidade e atos ilegais
Norma	1401 - Relatórios
Diretriz	2202 - Avaliação de Risco no Planejamento
Diretriz	2204 - Materialidade

Data de Vigência

Esta norma da ISACA é válida para todas as contratações de auditoria e garantia de SI a partir de 1º de novembro de 2013.