Norma 1202 de Auditoria e Garantia de SI Avaliação de Risco no Planejamento

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).

Norma 1202 de Auditoria e Garantia de SI - Avaliação de Risco no Planejamento

Declarações

1202.1 **A função de auditoria e garantia de SI deve usar uma abordagem de avaliação de risco e metodologia de suporte apropriada para desenvolver o plano de auditoria de SI geral e determinar prioridades para a alocação eficaz de recursos de auditoria de SI.**

1202.2 **Profissionais de auditoria e garantia de SI devem identificar e avaliar riscos relevantes para a área em análise ao planejar contratações individuais.**

1202.3 **Profissionais de auditoria e garantia de SI devem considerar o risco do assunto, o risco da auditoria e a exposição relacionada para a empresa.**

Aspectos principais

Ao planejar atividades contínuas, a função de auditoria e garantia de SI deve:

- Conduzir e documentar, pelo menos anualmente, uma avaliação de risco para facilitar o desenvolvimento do plano de auditoria de SI.
- Incluir, como parte da avaliação de risco, os planos e objetivos estratégicos organizacionais, e a estrutura e iniciativas de gestão de risco empresarial.
- Para cada contratação de auditoria e garantia de SI, quantificar e justificar a quantidade de recursos de auditoria de SI necessários para atender aos requisitos da contratação.
- Usar avaliações de riscos na seleção de áreas e itens de interesse de auditoria e nas decisões, para projetar e conduzir contratações de auditoria e garantia de SI específicas.
- Buscar aprovação da avaliação de risco com os interessados na auditoria, além de outras partes apropriadas.
- Priorizar e programar o trabalho de auditoria e garantia de SI com base na avaliação de risco.
- Com base na avaliação de risco, desenvolver um plano que:
  - Atue como uma estrutura para atividades de auditoria e garantia de SI
  - Considere requisitos e atividades que não sejam de auditoria e garantia de SI
  - Seja atualizado, pelo menos anualmente, e aprovado pelas pessoas encarregadas da governança.
  - Aborde responsabilidades definidas pela Carta de Auditoria

Ao planejar uma contratação individual, profissionais de auditoria e garantia de SI devem:

- Identificar e avaliar riscos relevantes para a área em análise.
- Conduzir uma avaliação preliminar do risco relevante para a área em análise, para cada contratação. Os objetivos de cada contratação específica devem refletir os resultados da avaliação preliminar de riscos.
- Ao considerar áreas de riscos e planejar uma contratação específica, considerar auditorias, análises e resultados anteriores, incluindo qualquer atividade de reparação. Considerar também o processo de avaliação de risco dominante do conselho.
- Tentar reduzir o Risco de Auditoria a um nível aceitável, e atender aos objetivos de auditoria através de uma avaliação adequada do assunto e de controles relacionados de SI, planejando e realizando, ao mesmo tempo, a auditoria de SI.

- Ao planejar um procedimento específico de auditoria de SI, reconhecer que, quanto menor o limite de materialidade, mais precisas serão as expectativas de auditoria e maior o risco de auditoria.
- Para reduzir o risco de maior materialidade, compensar estendendo o teste de controles (reduzir o risco de controle) e/ou estendendo os procedimentos de Testes Substantivos (reduzir o risco de detecção) para obter garantia adicional.

Termos

Termo	Definição
Carta de Auditoria	Um documento aprovado pelas pessoas encarregadas da governança, que define o objetivo, a autoridade e a responsabilidade da atividade de auditoria interna A carta deve: • Estabelecer a posição da função de auditoria interna na empresa • Autorizar o acesso a registros, pessoal e propriedades físicas relevantes para o desempenho de contratações de auditoria e garantia de SI • Definir o escopo de atividades da função de auditoria
Risco de auditoria	O risco de chegar a uma conclusão incorreta com base em resultados da auditoria. Os três componentes de risco da auditoria são: • Risco de controle • Risco de detecção • Risco inerente
Risco do assunto da auditoria	Risco relevante para a área em análise: • Risco comercial (capacidade do cliente de pagar, mérito do crédito, fatores de mercado etc.) • Risco de contrato (responsabilidade, preço, tipo, penalidades etc.) • Risco do país (política, ambiente, segurança etc.) • Risco do projeto (recursos, conjunto de habilidades, metodologia, estabilidade do produto etc.) • Risco de tecnologia (solução, arquitetura, rede de infraestrutura de hardware e software, canais de distribuição etc.) Consulte risco inerente.
Risco de controle	O risco de que um erro material exista, que não seria evitado ou detectado em tempo hábil pelo sistema de controle interno. (Consulte risco inerente.)
Risco de detecção	O risco de que procedimentos substantivos do profissional de auditoria ou garantia de SI não detectarão um erro que poderia ser material, individualmente ou em combinação com outros erros. Consulte risco de auditoria.
Risco inerente	O nível ou exposição de risco sem levar em conta as medidas que a gestão tomou ou pode tomar (por exemplo, a implementação de controles). Consulte risco de controle.

Materialidade	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 assunto específico no contexto da empresa, como um todo
Avaliação de risco	Um processo usado para identificar e avaliar riscos e seus efeitos potenciais Avaliações de riscos são usadas para identificar os itens ou as áreas que apresentam o maior risco, vulnerabilidade ou exposição para a empresa, para inclusão no plano de auditoria anual de SI. Avaliações de riscos também são usadas para gerenciar a entrega de projetos e o risco de benefício do projeto.
Testes substantivos	Obtenção de evidência de auditoria sobre a totalidade, precisão ou existência de atividades ou transações durante o período de auditoria.

Vinculação a diretrizes

Tipo	**Título**
Diretriz	2202 - Avaliação de Risco no Planejamento

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.

