Requisitos Temáticos

Orientação para a Aplicação



The Institute of
Internal Auditors

Orientação para a Aplicação dos Requisitos Temáticos

Conteúdos

1. O Papel do Julgamento Profissional
2. Uma Abordagem Baseada em Riscos para Determinar a Aplicabilidade
3. Requisitos Obrigatórios Relacionados à Identificação do Tema
4. Aplicando os Requisitos Temáticos no Ciclo de Vida da Auditoria
5. Limitações e Exclusões de Escopo
6. Abordando Áreas de Alto Risco Ainda Não Maduras
7. Restrições de Recursos
8. Alinhamento Regulatório e Uso de Outros Frameworks
9. Aplicando Múltiplos Requisitos Temáticos

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

Orientação para a Aplicação dos Requisitos Temáticos

O Framework Internacional de Práticas Profissionais® compreende as Normas Globais de Auditoria Interna™, os Requisitos Temáticos e as Orientações Globais. Os Requisitos Temáticos são obrigatórios para trabalhos de avaliação e recomendados para trabalhos de consultoria em áreas de risco específicas. Devem ser usados em conjunto com as Normas, que constituem a base fidedigna para as práticas exigidas.

Os Requisitos Temáticos fornecem uma base mínima consistente para a cobertura de áreas de risco específicas. Os auditores internos devem aplicar procedimentos adicionais quando riscos organizacionais, regulamentos ou o contexto exigir maior profundidade.

1. O Papel do Julgamento Profissional

A aplicação do julgamento profissional é essencial para usar os Requisitos Temáticos com eficácia e é explicitamente exigida pelas Normas. O julgamento profissional permite que os auditores internos **ajustem a aplicação do Requisito Temático ao contexto exclusivo, ao perfil de risco e às prioridades estratégicas da organização, garantindo que a cobertura da auditoria seja relevante e proporcional.**

O julgamento profissional é exercido em várias etapas do ciclo de vida da auditoria. Ele desempenha um papel durante o **processo de planejamento da auditoria interna,** conforme descrito na Norma 9.4 – Plano de Auditoria Interna, no qual são tomadas decisões sobre quais riscos relacionados ao Requisito Temático são significantes o bastante para justificar cobertura. Também é usado ao **definir o escopo e os objetivos** de um trabalho de acordo com a Norma 13.3 – Objetivos e Escopo do Trabalho, particularmente para determinar se o Requisito Temático deveria ser aplicado integralmente ou apenas em parte. Além disso, o julgamento é **aplicado ao avaliar e documentar a aplicabilidade e as exclusões,** ao selecionar critérios de avaliação (Norma 13.4 – Critérios de Avaliação) e as etapas do programa de trabalho (Norma 13.6 – Programa de Trabalho), e ao **decidir se as evidências de auditoria de prestadores externos de avaliação,** como auditorias regulatórias, atendem aos requisitos.

Embora a conformidade com os Requisitos Temáticos seja esperada, pode haver circunstâncias excepcionais, como restrições de recursos ou considerações específicas do setor, em que a conformidade total não seja viável. Nesses casos, o chefe executivo de auditoria deveria implementar ações alternativas que atinjam a intenção do requisito e deve documentar e comunicar a justificativa do desvio. Essa **abordagem de "cumprir ou explicar"** está alinhada aos princípios descritos nas Normas.

De acordo com o Princípio I das Normas, Propósito da Auditoria Interna, os auditores internos devem demonstrar integridade e objetividade ao usar o julgamento profissional. A Norma 4.1 –

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

Conformidade com as Normas Globais de Auditoria Interna exige que esse julgamento seja exercido com zelo profissional devido. Isso significa que as decisões devem ser fundamentadas e baseadas em evidências, e não arbitrárias ou intuitivas. Elas deveriam ser consistentes com a metodologia de auditoria interna e alinhadas às prioridades de risco da organização. **Todas as decisões baseadas em julgamento deveriam ser claramente documentadas** nos registros de planejamento da auditoria, nos papéis de trabalho ou nas matrizes de aplicabilidade do Requisito Temático, e **devem ser transparentes e defensáveis durante revisões de avaliação de qualidade ou avaliações externas.** A documentação reflete a importância de uma abordagem bem fundamentada e ponderada: demonstrar a conformidade se torna mais simples quando a justificativa está claramente documentada.

O julgamento profissional não substitui a estrutura; ele permite que os auditores internos **adaptem requisitos estruturados, como os Requisitos Temáticos, a realidades complexas.** O julgamento profissional garante que os esforços de auditoria estejam não apenas alinhados às Normas, mas também ajustados às necessidades da organização, entregando uma avaliação que seja ao mesmo tempo confiável e relevante.

2. Uma Abordagem Baseada em Riscos para Determinar a Aplicabilidade

As atividades de auditoria seguem uma abordagem baseada em riscos, para garantir que os recursos estejam concentrados nas áreas de maior significância. A identificação dos temas de auditoria e a determinação do escopo deveriam estar fundamentadas em uma avaliação de riscos minuciosa e bem documentada. Um Requisito Temático aplica-se quando o tema **é identificado durante essa avaliação de riscos e o risco excede um nível de risco significante.**

Para **avaliar a significância de um risco relacionado a um Requisito Temático,** a função de auditoria interna deveria primeiro identificar o risco com base nos objetivos estratégicos da organização, nas exposições conhecidas, nos incidentes passados ou nas mudanças ambientais. Em seguida, o risco inerente deveria ser avaliado, considerando seu impacto e sua probabilidade. Essa "pontuação de risco" pode, então, ser comparada ao apetite a risco definido da organização, para determinar se ela excede o limite crítico.[1]

A definição do limite crítico está relacionada ao apetite a risco da organização, que é moldado pelas contribuições do conselho e da alta administração. As considerações incluem impactos financeiros, jurídicos, regulatórios e de conformidade, e impactos qualitativos, como danos à reputação ou o não cumprimento de expectativas estratégicas ou éticas. A liderança fornece uma direção clara sobre quais tipos de risco são aceitos apenas até uma medida limitada ou são intoleráveis, mesmo com probabilidades mais baixas. Expectativas claras do conselho e da alta administração e um entendimento acordado sobre as classificações são essenciais para garantir julgamentos consistentes e alinhados aos riscos sobre a significância dos riscos.

---

1. Os auditores internos podem considerar o uso de uma ferramenta reconhecida de pontuação de risco, como a ferramenta *Enterprise and Business Process Risks* do The IIA.

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

Depois que um risco é identificado como significante, ele deveria ser **mapeado em relação ao Requisito Temático relevante e ao respectivo componente de governança, gerenciamento de riscos ou controles, para determinar quais requisitos se aplicam.** A relevância de todos os requisitos deveria ser revisada. Quando requisitos específicos forem considerados não aplicáveis com base na natureza, no contexto ou na causa raiz do risco, essas exclusões devem ser claramente documentadas, incluindo a justificativa para sua omissão. Por exemplo, se o risco decorre de uma falha na execução dos controles, e não da governança, apenas os componentes relacionados a controles podem ser relevantes. Isso garante que a auditoria esteja alinhada aos riscos e tenha o escopo definido de forma apropriada.

Por fim, **o julgamento profissional** deve ser aplicado para confirmar a aplicabilidade da decisão, e a decisão e a justificativa deveriam ser devidamente documentadas.

3. Requisitos Obrigatórios Relacionados à Identificação do Tema

Os Requisitos Temáticos são obrigatórios para trabalhos de avaliação quando o risco é identificado durante a avaliação de riscos e excede um limite crítico (consulte a seção 2, "Uma Abordagem Baseada em Riscos para Determinar a Aplicabilidade"). Isso pode se referir à avaliação de riscos periódica usada para elaborar o plano de auditoria e à avaliação de riscos específica realizada para definir o escopo de um trabalho de auditoria. Os Requisitos Temáticos são recomendados para trabalhos de consultoria quando o tema se relaciona aos objetivos do trabalho.

Os Requisitos Temáticos são aplicáveis **quando o tema está explicitamente incluído no plano de auditoria interna como um trabalho de avaliação.** A aplicação pode ocorrer por meio de uma auditoria temática abrangente, voltada inteiramente ao assunto, ou os requisitos podem ser abordados em vários trabalhos, possivelmente distribuídos ao longo de vários anos. Nesses casos, os auditores internos devem garantir que todos os requisitos relevantes sejam, por fim, cobertos e que a documentação do trabalho mostre claramente como e quando cada parte é abordada.

Os Requisitos Temáticos também devem ser aplicados **quando o tema é identificado durante um trabalho,** o que significa que o tema atingiu um nível priorizado acima do limite crítico, com base no apetite a risco da organização. Ele deveria ser tratado como um risco significante que exige atenção, em linha com os objetivos e a avaliação de riscos do trabalho. É importante destacar que nem todas as partes do Requisito Temático devem ser aplicadas se o risco identificado disser respeito apenas a um subconjunto de elementos de governança, gerenciamento de riscos e controle (p. ex., apenas controles ou governança). O escopo de aplicação deve estar alinhado à natureza e à extensão do risco identificado e aos objetivos da auditoria. O julgamento profissional deveria ser usado para determinar quais requisitos são relevantes e proporcionais ao nível e ao tipo de risco.

Um Requisito Temático também é **aplicável quando o tema passa a fazer parte de um trabalho incluído mediante solicitação,** mesmo que não tivesse sido originalmente incluído no plano de auditoria. Nesses casos, a aplicação do Requisito Temático ainda deve seguir uma abordagem baseada em riscos. Os auditores internos podem aplicar o conjunto completo ou

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

apenas um subconjunto dos requisitos, dependendo da materialidade do risco e de seu alinhamento com os limites de risco da organização.

4. Aplicando os Requisitos Temáticos no Ciclo de Vida da Auditoria

Depois que um risco é considerado significante por meio da avaliação de riscos e que um Requisito Temático é aplicável, os auditores internos deveriam aplicar o Requisito Temático de forma consistente ao longo do ciclo de vida da auditoria:

No Nível do Planejamento da Auditoria

Durante a elaboração do plano de auditoria, em linha com a Norma 9.4 – Plano de Auditoria Interna, os riscos relacionados a Requisitos Temáticos identificados como significantes deveriam ser refletidos de forma apropriada, incluindo **uma auditoria temática pontual *(standalone)* ou integrando os requisitos a vários trabalhos, possivelmente distribuídos ao longo de ciclos ou anos de auditoria.** Em ambos os casos, é importante mencionar claramente o Requisito Temático aplicável no universo de auditoria, na documentação da avaliação de riscos e nos registros de planejamento, para garantir transparência e alinhamento tanto com as prioridades organizacionais quanto com as normas profissionais.

Durante a Execução do Trabalho

Os auditores internos deveriam aplicar o julgamento profissional para ajustar a aplicação do Requisito Temático às características específicas do risco. A Norma 13.3 – Objetivos e Escopo do Trabalho inclui considerar a causa subjacente do risco e identificar quais elementos de governança, gerenciamento de riscos ou controle são mais relevantes para a manifestação e o impacto do risco. Com base nessa análise, **apenas os requisitos diretamente alinhados ao escopo e aos objetivos definidos do trabalho precisam ser aplicados.** Como resultado, certas partes do Requisito Temático podem ser excluídas de forma justificada quando estiverem fora do escopo do risco identificado e dos objetivos do trabalho. Essas exclusões deveriam refletir uma abordagem baseada em riscos e proporcional, e devem ser claramente documentadas nos papéis de trabalho, incluindo uma justificativa que demonstre o alinhamento com o foco do trabalho.

Os auditores internos deveriam, então, realizar o **trabalho de campo** para sustentar as conclusões sobre os requisitos aplicáveis, a fim de garantir uma cobertura significante e direcionada.

5. Limitações e Exclusões de Escopo

As decisões sobre aplicabilidade e exclusão são exigidas **assim que o tema é identificado como um risco significante ou priorizado,** mas essas decisões podem ser **documentadas em diferentes etapas do processo de auditoria.** Por exemplo, elas podem ser registradas no nível do plano de auditoria, quando o tema é coberto por um trabalho dedicado ou distribuído entre vários trabalhos ao longo do tempo. Alternativamente, podem ser documentadas no nível do trabalho, quando o tema é identificado durante o planejamento ou o trabalho de campo, ou quando os stakeholders solicitam cobertura.

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

As boas práticas de documentação envolvem aplicar uma lógica clara e defensável ao determinar e registrar o escopo da aplicação do Requisito Temático. As práticas incluem avaliar a **relevância do(s) requisito(s) aplicável(is), avaliando o contexto organizacional e as especificidades do risco identificado.** As exclusões ou aplicações parciais deveriam ser respaldadas por referências apropriadas, como classificações de risco, limitações de escopo, julgamento profissional aplicado e a justificativa para a cobertura selecionada. A documentação e justificativa sólidas ajudam os auditores a se sentirem confiantes quanto à sua cobertura e reduzem a dúvida de que algo tenha ficado de fora.

É importante destacar que uma **avaliação de riscos bem executada já deveria gerar grande parte da documentação exigida,** tornando esse processo parte integrante do planejamento da auditoria, e não um ônus administrativo. Além disso, essa documentação é essencial, pois será usada durante as **avaliações de qualidade** para avaliar se os Requisitos Temáticos foram aplicados de forma apropriada e consistente.

As ferramentas fornecidas no guia do usuário, como uma **matriz de aplicabilidade do Requisito Temático,** podem apoiar a consistência, a rastreabilidade e o alinhamento com as normas profissionais.

6. Abordando Áreas de Alto Risco Ainda Não Maduras

Quando um tema é identificado como uma área de alto risco, mas o nível de maturidade da organização na governança, gerenciamento de riscos e controle em torno dele é baixa, a função de auditoria interna continua sendo responsável por abordá-lo.

De acordo com as Normas, a função de auditoria interna deve garantir que os riscos significantes sejam levados ao conhecimento do **conselho e da alta administração**. É necessária uma conversa clara e franca para garantir que a liderança entenda que a área de risco contém exposições substanciais que atualmente não estão adequadamente cobertas pelas estruturas ou pelos processos existentes.

Nesses casos, o Requisito Temático pode servir, no contexto de um trabalho de consultoria, como orientação recomendada e fornecer um framework valioso para avaliar lacunas, destacar exposições e criar conscientização em toda a organização.

Mesmo que ainda não seja possível prestar uma avaliação completa, o papel da função de auditoria interna é garantir transparência, promover a conscientização e incentivar a gestão a assumir a propriedade da questão. Além disso, o assunto deveria ser escalado ao conselho, para garantir a conscientização e o alinhamento quanto à abordagem apropriada.

7. Restrições de Recursos

Se a função de auditoria interna não tiver a capacidade, como tempo, equipe ou orçamento, ou as competências necessárias para aplicar integralmente um Requisito Temático, incluindo conhecimento especializado no assunto ou habilidades técnicas, isso não dispensa a responsabilidade de avaliar o risco ou determinar sua aplicabilidade. De acordo com a Norma 8.2

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

– Recursos, **o chefe executivo de auditoria deve informar o conselho sobre essas limitações de recursos e explicar como elas serão abordadas.**

Em resposta às restrições de recursos, a função de auditoria interna **pode desenvolver capacidades internas** por meio de treinamento direcionado ou recrutamento. Alternativamente, ela pode terceirizar ou fazer *cosourcing* do trabalho com especialistas externos qualificados. Em alguns casos, a auditoria pode ter **o escopo redefinido,** mas somente quando essa decisão for respaldada por uma justificativa documentada e acordada ou aprovada pelo conselho.

O chefe executivo de auditoria é responsável por garantir a conformidade com o Requisito Temático e identificar opções para atingi-la, como a terceirização, mantendo a prestação de contas geral. Em casos de não conformidade, a auditoria interna deve garantir que isso **seja divulgado de forma transparente** juntamente com os motivos subjacentes, como limitações de recursos. Todas as ações de mitigação relacionadas devem ser claramente documentadas no plano de auditoria e nos arquivos dos trabalhos, mantendo a prestação de contas e a rastreabilidade durante todo o processo.

8. Alinhamento Regulatório e Uso de Outros Frameworks

Os Requisitos Temáticos são aplicáveis globalmente e estabelecem uma base mínima para a cobertura da auditoria interna de áreas de risco específicas, independentemente do tamanho, do setor ou da maturidade da organização. No entanto, as organizações também podem estar sujeitas a **requisitos regulatórios, normas ou frameworks externos,** como NIST, ISO 27001, relatórios SOC, leis e regulamentos ou obrigações específicas da indústria, que se sobrepõem ou vão além do escopo de um determinado Requisito Temático.

Espera-se que os auditores internos adotem uma **abordagem baseada em riscos e comparativa** quando isso ocorrer. Se um requisito regulatório ou framework externo impuser uma **obrigação mais rigorosa ou mais abrangente** do que a do Requisito Temático, esse padrão mais elevado deveria orientar o escopo da auditoria. De fato, a maioria dos frameworks regulatórios, particularmente em áreas de alto risco como cibersegurança, gestão de terceiros ou serviços financeiros, tende a ser mais detalhada e exigente do que o Requisito Temático correspondente. Assim, quando as organizações já estão em conformidade com essas normas mais rigorosas, demonstrar o alinhamento com o Requisito Temático geralmente não deveria exigir um esforço adicional significativo, desde que o vínculo seja documentado e a suficiência da cobertura seja avaliada.

O mapeamento do Requisito Temático em relação aos requisitos regulatórios e a outros frameworks reconhecidos é considerado uma boa prática. O mapeamento permite que a função de auditoria interna demonstre como os requisitos estão sendo atendidos — diretamente ou por meio da confiança em evidências de auditorias regulatórias existentes —, ao mesmo tempo que garante que nenhuma lacuna crítica seja ignorada. Por exemplo, se uma auditoria de cibersegurança já tiver sido realizada com base nas orientações do NIST por outro prestador de avaliação, a função de auditoria interna pode fazer referência a esse trabalho e aproveitá-lo para confirmar o alinhamento com o Requisito Temático de Cibersegurança. No entanto, isso deve ser documentado de forma explícita e a suficiência das evidências deveria ser avaliada com o uso do

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

julgamento profissional (consulte também o Guia Prático Global *Coordenação e Confiança: Trabalhando com Outros Prestadores de Avaliação*).

Em última análise, aplicar os Requisitos Temáticos em um ambiente regulado exige **coordenação cuidadosa.** Os auditores internos deveriam garantir que sua abordagem reflita a norma aplicável mais rigorosa, evitando duplicações e aproveitando controles, avaliações e auditorias externas existentes, quando apropriado. Isso apoia a eficiência e a credibilidade e garante que a auditoria interna continue cumprindo sua responsabilidade, de acordo com as Normas, de prestar **avaliação independente e baseada em riscos** que seja ao mesmo tempo **consciente do contexto e globalmente consistente**.

9. Aplicando Múltiplos Requisitos Temáticos

Aplicar múltiplos Requisitos Temáticos em um único trabalho de auditoria depende inteiramente dos riscos significantes específicos identificados por meio **do processo de avaliação de riscos da organização.** Em vez de presumir que vários Requisitos Temáticos deveriam ser aplicados em conjunto por padrão, os auditores internos devem avaliar se a natureza e o escopo do risco realmente exigem o uso de mais de um Requisito Temático.

Por exemplo, se um risco significante for identificado na área de cibersegurança de terceiros quando um terceiro presta serviços de cibersegurança, pode ser apropriado aplicar tanto o Requisito Temático de Cibersegurança quanto o Requisito Temático de Terceiros. No entanto, se o risco se referir exclusivamente à conformidade contratual de terceiros, sem implicações de cibersegurança, somente o Requisito Temático de Terceiros se aplicaria. Isso garante que o escopo da auditoria permaneça **direcionado aos riscos priorizados e evita qualquer expansão desnecessária da cobertura.**

Os auditores internos deveriam definir claramente o escopo **com base nos riscos significantes identificados,** para evitar a expansão do escopo da auditoria *(scope creep)* — em que a auditoria pode se estender inadvertidamente além de seus objetivos originais. Os objetivos da auditoria deveriam estar alinhados ao apetite a risco, à estratégia, aos objetivos e às prioridades da organização. A justificativa para incluir ou excluir Requisitos Temáticos específicos deveria ser documentada nos registros de planejamento do trabalho. Essa abordagem disciplinada ajuda a proteger a integridade do processo de auditoria, garante o uso eficiente de recursos e entrega uma avaliação focada nos riscos mais prementes da organização.

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.

Sobre o The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) é uma associação profissional internacional que atende a mais de 265.000 membros globais e concedeu mais de 200.000 certificações *Certified Internal Auditor*® (CIA®) no mundo todo. Criado em 1941, o The IIA é reconhecido no mundo todo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica.
Para mais informações, visite theiia.org.

Isenção de Responsabilidade

The IIA publica este documento para fins informativos e educacionais. Este material não tem o objetivo de fornecer respostas definitivas a circunstâncias individuais específicas e, assim, deve ser usado apenas como guia. The IIA recomenda a busca de assessoria especializada independente, relacionada diretamente a qualquer situação específica. The IIA não aceita qualquer responsabilidade pela confiança depositada unicamente neste material.

Copyright

© 2025 The Institute of Internal Auditors, Inc. Todos os direitos reservados. Para permissão para reprodução, favor contatar copyright@theiia.org.

Agosto de 2025

The Institute of Internal Auditors

Sede Global
1035 Greenwood Blvd., Suíte 401
Lake Mary, FL 32746, EUA
Tel.: +1-407-937-1111
Fax: +1-407-937-1101

 ©2025 The Institute of Internal Auditors. Todos os direitos reservados. Exclusivo para uso individual.