AVALIAÇÃO DE RISCOS NO PLANEJAMENTO DE AUDITORIA

Um *guia* para auditores sobre a melhor forma de avaliar riscos ao planejar o trabalho de auditoria

IA COP
INTERNAL AUDIT COMMUNITY OF PRACTICE

AVALIAÇÃO DE RISCOS NO PLANEJAMENTO DE AUDITORIA

Um *guia* para auditores sobre a melhor forma de avaliar riscos ao planejar o trabalho de auditoria

Abril de 2014

Índice

Prefácio

Este modelo é o produto de um processo de troca de ideias e informações entre os membros da Comunidade de Prática de Auditoria Interna (IA CoP), da rede PEM-PAL (Aprendizagem Assistida por Colegas sobre a Gestão de Despesas Públicas).

A rede PEM-PAL, lançada em 2006 com a ajuda do Banco Mundial, é um órgão regional que visa apoiar as reformas nas despesas públicas e na gestão financeira em vinte e um países da Ásia Central e Europa Central, promovendo a capacitação e a troca de informações. A IA CoP, uma das três comunidades de prática em torno da qual a rede está organizada, tem representantes de 21 países da região da Europa e Ásia Central.

Um dos objetivos da IA CoP é "contribuir para a melhoria dos sistemas de Gestão Financeira Pública (GFP), apoiando os membros a estabelecerem um Serviço de Auditoria Interna moderno e eficaz em seus Governos, que atenda às normas internacionais e da União Europeia (UE) e facilite a boa governança em seu setor público..."1 As atividades da IA CoP contribuem para promover essa agenda, oferecendo um guia na avaliação de riscos no planejamento de auditoria, que os auditores internos do setor público podem seguir como uma boa prática.

Este guia de Avaliação de Risco no Planejamento de Auditoria é o resultado final de um processo colaborativo de membros regionais e parceiros doadores, iniciado com um workshop realizado em Lvov, na Ucrânia, em outubro de 2012. A rede PEM-PAL e a IA CoP esperam que os usuários deste guia e de outros documentos da série encontrem informações úteis nos mesmos, para o avanço das reformas da auditoria interna do setor público.

1 Fonte: Classificação Equilibrada da IACOP

Agradecimentos

Este modelo foi o esforço conjunto de vários indivíduos e membros do Grupo de Trabalho para Avaliação de Riscos da Comunidade de Prática de Auditoria Interna (IA CoP) que compartilharam seu tempo e conhecimento para torná-lo realidade.

Especialmente, a IA CoP gostaria de reconhecer os seguintes principais colaboradores:

Stanislav Bychkov, Federação Russa, Co-líder do Grupo de Trabalho sobre Avaliação de Riscos

Ruslana Rudnitska, Academia Nacional de Finanças e Economia, Holanda

Richard Maggs, Banco Mundial, Consultor

Manfred van Kesteren, Academia Nacional de Finanças e Economia, Holanda

Grigor Aramyan, Armênia, Líder do Grupo de Trabalho em Avaliação de Riscos

Edit Németh, Hungria, Co-líder do Grupo de Trabalho sobre Avaliação de Riscos e Vice-Presidente Interina da IA CoP

Dorotea Manolova, Bulgária, Co-líder do Grupo de Trabalho sobre Avaliação de Riscos

Diana Grosu-Axenti, Moldávia, ex-Presidente da IA CoP

Arman Vatyan, Banco Mundial, Coordenador da IA CoP

As seguintes pessoas investiram esforços importantes no estabelecimento e operação inicial do Grupo de Trabalho para Avaliação de Riscos:

Joop Vrolijk, OCDE/SIGMA

Albana Gjinopulli, Albânia, ex-Líder do Grupo de Trabalho sobre Avaliação de Riscos

Acrônimos

CHU	Unidade Central de Harmonização
COSO	Comitê das Organizações Patrocinadoras da Comissão Treadway
GRC	Gestão de Riscos Corporativos
UE	União Europeia
CAI	Chefe de Auditoria Interna
AI	Auditoria Interna
IA CoP	Comunidade de Prática de Auditoria Interna
IIA	Instituto de Auditores Internos
TI	Tecnologia da Informação
PEM-PAL	Aprendizagem Assistida por Colegas sobre a Gestão de Despesas Públicas
ARP	Avaliação de Riscos no Planejamento de Auditoria
ONU	Organização das Nações Unidas
BM	Banco Mundial

Introdução

Fundamento e objetivo do guia

1. O guia Avaliação de Riscos no Planejamento de Auditoria (ARP), elaborado pela Comunidade de Prática de Auditoria Interna (IA CoP) da PEM-PAL, enfatiza a importância e o impacto que uma estratégia de auditoria eficaz e um plano de auditoria representam para a consecução das metas, objetivos e a missão da unidade de auditoria interna. O planejamento fornece uma abordagem sistemática ao trabalho de auditoria interna e requer conhecimento que abranja uma ampla gama de questões na gestão pública, incluindo a avaliação de riscos e o controle interno.

2. Este guia ARP foi desenvolvido para:

   - Ajudar as unidades de Auditoria Interna a produzir planos anuais efetivos e estratégicos, baseados em riscos.
   - Fornecer uma orientação sobre o planejamento e a avaliação de risco que possa ser usada como um conjunto de princípios pelas unidades centrais responsáveis por assessorar o desenvolvimento da Auditoria Interna em seus próprios países.

3. O guia é totalmente consistente com as Normas Internacionais do Instituto de Auditores Internos (IIA) para a Prática Profissional de Auditoria Interna no planejamento do trabalho de auditoria interna. Em particular:

   - A Norma IIA 2010, que exige que "o Chefe Executivo de Auditoria[1] deve estabelecer planos baseados em risco para determinar as prioridades da auditoria interna".
   - A Norma IIA 2010.A1, que exige que "o plano de trabalhos da atividade de auditoria interna deve se basear em uma avaliação de risco documentada, realizada pelo menos anualmente. A contribuição da alta administração e do conselho deve ser considerada neste processo".
   - A Norma IIA 2010.A2 "O Chefe Executivo de Auditoria deve identificar e considerar as expectativas da alta administração, do conselho e de outras partes interessadas em relação a pareceres de auditoria interna e outras conclusões."
   - A Norma IIA 2020, "O Chefe Executivo de Auditoria deve comunicar os planos da atividade de auditoria interna e os requisitos de recursos, incluindo mudanças intermediárias significativas, à alta administração e ao conselho para revisão e aprovação. O Chefe Executivo de Auditoria também deve comunicar o impacto das limitações de recursos."

4. Essas normas exigem que o Chefe de Auditoria Interna (CAI)[2] desenvolva um plano baseado em riscos. O CAI deve levar em consideração a estrutura de Gestão de Riscos da organização, incluindo os níveis de Apetite de riscosestabelecidos pela administração para as diferentes atividades ou partes da organização. Se não existir uma estrutura de Gestão de Riscos, o CAI usa seu próprio julgamento de riscos após considerar as informações da alta administração e do conselho. O CAI deve revisar e ajustar o plano, conforme necessário, em resposta a mudanças nos negócios, riscos, operações, programas, sistemas e controles da organização.

1 O Chefe Executivo de Auditoria é referido como Chefe de Auditoria Interna para os fins deste instrumento, que é um termo mais relevante para o setor público, conforme acordado pela IA CoP.

2 Ou um indivíduo designado para implementar esse cargo.

Por que o planejamento baseado em riscos é importante para uma unidade de auditoria interna

5. O principal desafio enfrentado pela maioria dos auditores internos é como alocar recursos limitados de auditoria interna da maneira mais eficaz - como escolher os assuntos de auditoria a serem examinados. Isso requer uma avaliação do risco em todas as áreas auditáveis que um auditor pode examinar.
6. O objetivo do planejamento baseado em riscos é garantir que o Auditor examine os assuntos de maior risco para a consecução dos objetivos da organização.
7. Os planos de auditoria estratégicos e anuais devem ser desenvolvidos por meio de um processo que identifique e priorize possíveis tópicos de auditoria. Toda a população de áreas auditáveis em potencial, que podem ser categorizadas de várias maneiras, é chamada **universo de auditoria**[3]. Para cada elemento do universo de auditoria, os riscos ou oportunidades devem ser avaliados e as decisões tomadas sobre outros fatores de risco que podem influenciar a prioridade a ser dada a cada elemento do universo de auditoria (**objetos de auditoria**).
8. Os planos estratégicos e anuais são documentos importantes, que normalmente são apresentados à administração. O plano estratégico oferece uma oportunidade para apresentar o trabalho do auditor interno e os benefícios que surgirão da função de auditoria. Representa uma vitrine, o que explica o que a auditoria interna pode fazer pela administração. O plano anual converte o plano estratégico nas atribuições de auditoria a serem realizadas no ano atual. Os planos estratégicos e anuais devem ser claramente estruturados e bem escritos e devem fornecer à administração um resumo persuasivo da lógica que apoia os julgamentos feitos sobre a prioridade dada a determinados tópicos. Uma abordagem estruturada do planejamento baseado em riscoss é um passo importante para uma estratégia de auditoria eficaz.

Como usar o guia

9. O guia ARP é apresentado em cinco capítulos da seguinte forma:
   - O Capítulo 1 “Compreendendo o planejamento de auditoria baseado em riscos” considera os recursos fundamentais do planejamento baseado em riscos e a estrutura conceitual usada no guia.
   - O capítulo 2 “Categorizando o universo de auditoria para o planejamento baseado em riscos” considera como

   categorizar o universo de auditoria para o planejamento baseado em riscoss.
   - O Capítulo 3 “Identificando riscos e avaliando sua probabilidade e impacto” considera como identificar e avaliar riscos em termos de probabilidade e impacto nos objetivos da organização.
   - O capítulo 4, “Construindo planos estratégicos e anuais com base no risco”, considera como usar fatores de risco e critérios de pontuação para identificar objetos de auditoria para inclusão nos planos estratégicos e anuais de auditoria.
   - O capítulo 5, “Escrevendo e atualizando planos estratégicos e anuais”, considera como desenvolver planos estratégicos e anuais e como mantê-los atualizados.
10. O guia contém orientações genéricas e também inclui:
    - Exemplos extraídos de pesquisas genéricas sobre práticas de auditoria interna;
    - Exemplo de práticas nos países da PEM-PAL (coletadas por meio de uma pesquisa); e
    - Várias dicas e sugestões gerais sobre questões-chave - esse é o tipo de suporte que um auditor experiente passaria para um colega menos experiente.

Dicas e sugestões gerais são apresentadas em caixas laranja.

3 Vide Capítulo 3

Capítulo 1. Compreendendo o planejamento de auditoria baseado em riscos

O que são riscos?

11. As principais definições relativas a risco são:

- Evento - um incidente ou ocorrência, de fontes internas ou externas a uma organização, que podem afetar a consecução dos objetivos. Eventos podem ter impacto negativo, impacto positivo ou ambos. Eventos com impacto negativo representam riscos. Eventos com impacto positivo representam oportunidades.
- Risco é a possibilidade de um evento ocorrer e afetar adversamente a conquista de objetivos. O risco é medido em termos de impacto e probabilidade.
- Oportunidade é a possibilidade de um evento ocorrer e afetar positivamente a realização de objetivos.
- Riscos principais são esses riscos que, se gerenciados adequadamente, tornarão a organização bem-sucedida na consecução de seus objetivos ou, se não for bem gerenciada, ela (a organização) não alcançará seus objetivos.
- Risco inerente é o nível de risco antes que quaisquer ações de mitigação de risco, como atividades de controle, sejam levadas em consideração (por exemplo, o risco inerente de inundação antes de levar em conta medidas de prevenção de inundação).
- Risco residual é o nível de risco após levar em consideração ações de mitigação de risco, como atividades de controle. O auditor está mais preocupado com o nível de risco residual. (Em alguns casos, o risco inerente e residual será o mesmo, mas as áreas bem controladas geralmente terão níveis mais baixos de risco residual.)
- Apetite de riscos é o nível de risco que uma organização está disposta a aceitar na busca de seus objetivos.
- Fatores de risco – um termo usado para descrever fatores genéricos que podem indicar um maior nível de risco e/ou prioridade a ser dada a um elemento do universo de auditoria.

Compreendendo as diferenças entre gestão e avaliação de riscos no planejamento de auditoria

12. Os riscos são considerados por gerentes e auditores e são definidos da mesma forma[4].

- A Gestão de Riscos é (ou deveria ser) parte integrante do sistema de controle interno[5] e é de responsabilidade da administração. É um processo estruturado em que os gerentes (a) examinam prováveis eventos futuros e os riscos e as oportunidades que eles representam para a consecução dos objetivos da organização; e (b) determinam e implementam ações de Gestão de Riscos (por exemplo, atividades de controle).
- A avaliação do risco de auditoria faz parte do planejamento e de um processo em que os auditores consideram (i) os eventos individuais, os riscos e as oportunidades que os mesmos representam para a consecução dos objetivos dos elementos do universo de auditoria e (ii) fatores de riscos genéricos

4 Nota: os auditores também devem considerar o “Risco de auditoria”, que é um risco específico que surge devido à natureza seletiva do trabalho de auditoria - a possibilidade de que os resultados de uma auditoria não estejam corretos.

5 Consulte as orientações sobre controle interno produzidas pelo Comitê das Organizações Patrocinadoras da Comissão Treadway (COSO) para obter mais informações sobre o vínculo entre gestão de riscos e controle interno.

que ajudam a priorizar o trabalho em áreas de maior risco. O objetivo da avaliação de risco de auditoria é garantir que os recursos sejam direcionados à auditoria das áreas de maior risco para a organização.

☑ **Ninguém pode avaliar o risco, se os objetivos não forem claros**. Se não estiver claro o que um elemento do universo de auditoria está tentando alcançar, você não poderá realizar uma avaliação de risco. Certifique-se de entender os objetivos de diferentes elementos do universo de auditoria antes de tentar identificar eventos prováveis que impactam esses objetivos e os riscos inerentes e residuais envolvidos.

Os padrões de auditoria afirmam claramente que, onde a administração possui um sistema de Gestão de Riscos em funcionamento, os auditores devem usá-lo como base para realizar sua própria avaliação de risco.

13. Embora a Gestão de Riscos seja um processo lógico, muitas organizações do setor público não tratam a Gestão de Riscos de maneira consistente e estruturada e não possuem controle interno eficaz. Nessa situação, os auditores devem fazer seus próprios julgamentos sobre riscos dentro da organização. Em outras palavras: o auditor deve avaliar os riscos para a consecução dos objetivos da organização, mesmo que a administração não avalie.

☑ Se existir um forte processo de Gestão de Riscos, o mesmo poderá ser revisado pela auditoria interna (AI) como parte de seu processo de planejamento anual.

☑ Mesmo quando a AI precisa realizar sua própria avaliação de risco, ela busca informações da administração sobre coisas como o apetite da organização por riscos.

☑ Uma AI dos processos de gestão de riscos conduzidos para incentivar uma melhor gestão de riscos na organização pode frequentemente ser uma auditoria muito produtiva para um auditor interno.

Uma estrutura conceitual para o planejamento de auditoria baseado em riscos

14. Para desenvolver um plano baseado em riscos, o auditor precisa considerar dois aspectos do risco:
    (a) eventos/riscos individuais e como eles podem impactar a realização dos objetivos da organização (Vide Capítulo 3); e

    (b) fatores de risco genéricos que podem sugerir um nível de risco mais alto ou mais baixo e que podem ser usados para determinar a prioridade que deve ser dada a uma única auditoria no universo de auditoria.

15. Quando uma organização já implementou processos de Gestão de Riscos, o auditor pode examinar os registros de riscos para ver quais riscos individuais foram identificados pela administração e as medidas tomadas para trata-los. Onde não houver um processo de Gestão de Riscos, o auditor precisará identificar possíveis eventos que possam gerar riscos e avaliá-los em termos de impacto e probabilidade.

16. A estrutura conceitual básica para o planejamento de auditoria baseado em riscos possui, portanto, cinco estágios distintos:

    1. Determinar e categorizar o universo de auditoria. (Vide Capítulo 2)
    2. Identificar eventos individuais que podem dar origem a riscos e oportunidades em todo o universo de auditoria. (Vide Capítulo 3)
    3. Marcar eventos em termos de probabilidade e impacto (levando em consideração as ações de gerenciamento para mitigar o risco) para identificar o nível de risco residual. (Vide Capítulo 3)

4. Construir planos de auditoria baseados em risco usando fatores de risco genéricos e critérios de pontuação para cada fator para determinar a prioridade da auditoria de todos os objetos de auditoria no universo de auditoria. (Vide Capítulo 4)
5. Apresentar os resultados do planejamento baseado em riscoss, escrevendo e atualizando planos de trabalho estratégicos e anuais. (Vide Capítulo 5)

Levando em conta os processos de Gestão de Risco de Entidades

17. O processo de planejamento deve considerar até que ponto a administração já avaliou o risco e quais elementos comuns dessa avaliação o auditor pode usar. A Tabela 1 abaixo compara os elementos comuns da Gestão de Riscos com um processo típico de avaliação de riscos no planejamento de auditoria.

Tabela 1 - Os elementos comuns da gestão de riscos e planejamento de auditoria com base em riscos

Etapas de Gestão de Riscos	Etapas do planejamento de auditoria baseado em riscos
Os objetivos devem ser estabelecidos pela administração antes de realizar uma avaliação de risco.	
1. Identificação de eventos que possam dar origem a riscos e oportunidades para a consecução de objetivos.	1. Determinar e categorizar o universo de auditoria.
2. Marcar eventos em termos de probabilidade e impacto para identificar o nível de risco **inerente**.	2. Identificar eventos que podem dar origem a riscos e oportunidades em todo o universo de auditoria. Este é essencialmente o mesmo processo, mas está relacionado ao universo de auditoria.
	*O auditor estará muito interessado em saber como a administração avaliou o risco **inerente**, mas a principal preocupação para fins de planejamento é o risco **residual**. Portanto, esta revisão deve levar em consideração as etapas 3 e 4 da Gestão de Riscos.*
	Os auditores não são responsáveis por determinar a resposta ao risco, mas podem ter pareceres sobre sua eficácia. (Por exemplo, os gerentes podem considerar que não é necessário controlar um risco específico, enquanto o auditor pode pensar que seria melhor fazê-lo.)
	Os auditores não são responsáveis por implementar ações de mitigação e devem avaliar a eficácia das atividades de controle em termos de seu impacto no risco residual.
3. Determinação de uma resposta de risco apropriada (se aceita ou não o risco, transfere o risco para outras pessoas ou controla o risco).	3. Pontuação de eventos em termos de probabilidade e impacto (levando em consideração as ações de gerenciamento para mitigar riscos) para identificar o nível de risco **residual**.

Etapas de Gestão de Riscos	Etapas do planejamento de auditoria baseado em riscos
4. Implementação da ação de mitigação de risco decidida para atingir um nível aceitável de risco residual - isso inclui atividades de controle.	4. Desenvolver fatores de riscos genéricos e critérios para cada fator, com a finalidade de identificar a prioridade dos objetos de autoria contidos no universo auditável.
	5. Desenvolvimento e manutenção de planos de auditoria baseados em risco (plano estratégico e plano de trabalho anual).

Na tabela, fica claro que há uma sobreposição significativa entre os dois primeiros estágios da Gestão de Riscos e os segundo e terceiro estágios da avaliação de riscos do planejamento de auditoria.

19. A principal diferença é que os gerentes precisam avaliar riscos **inerentes** para que possam determinar e implementar ações de mitigação de riscos (incluindo controles). Entretanto, o auditor precisa avaliar o risco **residual** (que é o risco que permanece após a efetividade dos controles internos) para determinar as áreas que são de alta prioridade para o exame.

20. Um exemplo simples ilustra a relação entre risco inerente, atividades de controle e risco residual: *se você atravessar a rua, há um número quase infinito de riscos inerentes. Um dos riscos inerentes, com alta probabilidade e grande impacto, é ser atropelado por um carro. Portanto, para atenuar esse risco, implementamos o controle de olhar à esquerda e à direita para verificar o tráfego que se aproxima antes de atravessar a rua. Mas isso não eliminará todos os riscos possíveis e os riscos residuais permanecem. Por exemplo, você ainda pode ser atingido por um meteoro porque não olhou para cima!*

21. A razão para isso é óbvia. Com recursos limitados, o auditor deseja concentrar o trabalho de auditoria nas áreas em que a organização está mais exposta ao risco.. Se o risco inerente for muito alto, mas existirem bons controles, o risco residual pode ser baixo e, portanto, não é digno de exame.

Entenda a diferença entre risco inerente e residual:

Risco inerente - atividades de controle = risco residual.
O foco do auditor no planejamento baseado em riscos está na identificação de altos níveis de risco residual.
Se uma organização for nova e/ou não houver informações sobre a eficácia das atividades de controle, a situação é a seguinte:
Risco inerente = risco residual

As ações necessárias para implementar o planejamento baseado em riscos

22. A tabela abaixo mostra as principais ações necessárias para implementar a estrutura conceitual do planejamento com base em riscos e como isso seria diferente para organizações com ou sem sistemas de Gestão de Riscos em vigor.

Etapas do planejamento de auditoria baseado em riscos	Gestão de Riscos em vigor	Sem Gestão de Riscos em vigor
1. Determinar e categorizar o universo de auditoria. ***(Vide Capítulo 2)***	✓ *Identificar categorias para dividir o universo de auditoria em objetos auditáveis discretos.* ✓ *Discutir e concordar com a administração a abordagem da categorização.* ✓ *Identificar e listar todos os objetos de auditoria em seu universo de auditoria por categoria acordada.*	
2. Identificar eventos que podem causar o aumento de riscos e oportunidades em todo o universo de auditoria. ***(Vide Capítulo 3)***	✓ *Revise os registros de risco para entender os eventos que os gerentes identificaram.* ✓ *Considerar a totalidade dos eventos identificados e discutir com os gerentes seus pareceres sobre o apetite de risco da organização.*	✓ *Identificar eventos que podem dar origem a riscos e oportunidades em todo o universo de auditoria.* ✓ *Discutir os riscos e as oportunidades com os gerentes para obter pontos de vista sobre a integridade e discutir com os gerentes seus pontos de vista sobre o apetite por riscos da organização.*
3. Marcar eventos em termos de probabilidade e impacto (levando em consideração as ações de gerenciamento para mitigar riscos) para identificar o nível de risco residual. (Vide Capítulo 3)	✓ *Revisar a maneira como a administração classificou os eventos e as ações implementadas para lidar com os principais riscos.* ✓ *Considerar a eficácia das ações de mitigação de riscos em termos de seu impacto nos riscos residuais.* ✓ *Identificar altos níveis de risco residual que precisam ser considerados nos planos de trabalho estratégicos e anuais.*	✓ *Classificar os eventos em termos de probabilidade e impacto (levando em consideração as ações de gerenciamento para mitigar o risco) para identificar o nível de risco residual.* ✓ *Discutir a abordagem com os gerentes e obter acordo sobre a maneira como os riscos estão sendo pontuados.*
4. Desenvolver fatores de riscos genéricos e critérios para cada fator, com a finalidade de identificar a prioridade dos objetos de autoria contidos no universo auditável. ***(Vide Capítulo 4)***	✓ *Produzir lista inicial de fatores de risco.* ✓ *Determinar critérios para pontuar cada fator de risco.* ✓ *Decidir se deseja adicionar uma ponderação a cada fator de risco.* ✓ *Discutir a abordagem com a administração e obter seus pareceres sobre a relevância dos fatores de risco escolhidos, os critérios a serem usados na pontuação e a ponderação a ser dada.* ✓ *Classificar cada fator de risco para identificar prioridades altas , médias e altas para todos os objetos de auditoria no universo de auditoria.*	

Etapas do planejamento de auditoria baseado em riscos	Gestão de riscos em vigor	Não há gestão de riscos em vigor
5. Desenvolvimento e manutenção de planos de auditoria baseados em risco (plano estratégico e plano de trabalho anual). ***(Vide Capítulo 5)***	✓ *Determinar a estratégia e os ciclos de cobertura para diferentes categorias do universo de auditoria, com base nas pontuações dos fatores de risco.* ✓ *Desenvolver um documento de estratégia que suporte as escolhas feitas e explique a metodologia usada e os julgamentos feitos para chegar às decisões.* ✓ *Desenvolver um plano de trabalho anual, de acordo com a estratégia identificada, as auditorias específicas a serem realizadas, seus títulos, época e duração esperada.*	

Capítulo 2. Categorizando o universo de auditoria para o planejamento baseado em riscos

O que é "universo da auditoria"?

23. O Modelo de Manual de Auditoria Interna de Boas Práticas da IA CoP explica que o universo de auditoria é o "ponto de partida para o plano de auditoria interna" e define o universo de auditoria como: "O escopo geral da função de auditoria interna e a totalidade dos processos, funções e locais auditáveis".
    - A frase "universo de auditoria" é uma maneira simples de se referir à totalidade de todas as coisas que um auditor interno poderia examinar separadamente.
    - O universo consiste na totalidade de "objetos auditáveis", que é uma maneira de identificar e descrever parte distinta do negócio, sistema ou processo, que pode ser auditado separadamente. Objetos auditáveis precisam ser grandes o suficiente para justificar uma auditoria e pequenos o suficiente para serem gerenciáveis.

A abordagem do elefante - cortando o universo da auditoria em pequenos pedaços

24. A resposta para a questão: "Como comer um elefante?" é "Uma mordida de cada vez". É assim que precisamos tratar o universo de auditoria, cortando-o em sistemas, processos, programas ou unidades organizacionais específicos que podem ser auditados - **objetos auditáveis**.

25. Tradicionalmente, os objetos auditáveis eram categorizados pela estrutura organizacional e definidos de cima para baixo - uma análise **"vertical"**. Geralmente, um objeto auditável é igual a uma ou várias unidades organizacionais. Continua sendo um primeiro corte útil do universo de auditoria que a maioria das unidades de AI utiliza.

26. No entanto, essa pode não ser a maneira mais eficaz de planejar todas as auditorias possíveis. Portanto, também é importante projetar a cobertura de auditoria a partir de uma visão **horizontal** ou **multifuncional** da organização - ou seja, auditorias "horizontais" baseadas em processos de negócios inteiros. Por exemplo, pode-se dizer que os sistemas de contabilidade ou gerenciamento de negócios de uma organização operam horizontalmente porque afetam todas as unidades organizacionais. Esses sistemas podem representar riscos graves em vários processos e, portanto, devem ser examinados horizontalmente.

27. Normalmente, o universo de auditoria é uma mistura de várias fatias de cima para baixo (vertical) e multifuncionais (horizontais). A compra é frequentemente uma atividade-chave multifuncional. No entanto, pode ser dividida para fins de auditoria em local e tipo de compra. No Programa Mundial de Alimentos da ONU, por exemplo, as compras poderiam ser divididas em quatro objetos de auditoria: compras na sede, compras nos escritórios locais, compras de alimentos e compras de itens não-alimentares. Isso seria apropriado porque cada elemento possui regras, regulamentos e controles internos diferentes.

28. Existe um alto grau de semelhança na maneira como as unidades de AI no governo tipicamente cortam ou categorizam o universo de auditoria (veja exemplos de boas práticas abaixo e o Anexo C, por exemplo, dos países da PEM-PAL).

Tabela 2 - Exemplo de boas práticas de categorização do universo de auditoria

Da pesquisa de governo do IIA
1. Quase todas as unidades de AI têm um universo de auditoria formalmente documentado (97%)
2. As categorizações mais comuns usadas são:
• Departamentos - 97%
• Processos - 97%
• Unidade organizacional ou local - 81%
• Programas operacionais - 75%
• Linhas de serviço - 58%
• Portfólio de risco GRC - 28%
• Outros - 22%

29. Por fim, cabe ao CAI decidir como categorizar o universo de auditoria e quantas fatias faz sentido usar. Portanto, a maioria das unidades de AI deseja considerar o seguinte como as categorizações mínimas necessárias:

- Por estrutura organizacional (Departamentos, Divisões, Unidades, Projetos Independentes);
- Por processos comuns (Pagamentos, Recebimentos, Gestão de ativos, Compras, Contratação, Inventário, Gestão de Recursos Humanos);
- Por local (Sede, Escritórios Regionais, Escritórios Locais);
- Por programas operacionais (por exemplo, em uma agência ou departamento de transporte, podem incluir: construção de novas estradas, manutenção de estradas, emissão de licenças para motoristas, cobrança de multas por excesso de velocidade, etc.);
- Por linhas de serviço (por exemplo, em um departamento de previdência social, pode incluir: serviços para idosos, serviços para deficientes, serviços para atendimento de crianças, que podem ser administrados por vários departamentos ou unidades diferentes).

Exemplo - Auditoria interna da Organização das Nações Unidas para Agricultura e Alimentação

O universo de auditoria do gabinete consiste em cerca de 100 entidades auditáveis, divididas em 14 categorias: 1) Governança, 2) Reformas, 3) Gestão estratégica, 4) Iniciativas/Projetos EspecIIAs, 5) Planejamento e Orçamento, 6) Ciclo de Programa de Campo, 7) Sedes descentralizadas, 8) Sistemas e Tecnologia da Informação, 9) Conhecimento e Comunicação, 10) Segurança e Proteção, 11) Recursos Humanos, 12) Gestão Financeira, 13) Compras, Gestão de Propriedades e Instalações e 14) Serviços Administrativos e Outros.

☑ ***Possíveis fontes de informação para categorizar o universo de auditoria**:*

- ✓ *Informações de gestão que detalham metas, objetivos e alvos;*
- ✓ *Guias dos serviços da organização;*
- ✓ *Organogramas ou diretório do escritório;*
- ✓ *Relatórios anuais e quaisquer metas de desempenho definidas para a organização;*
- ✓ *Planos corporativos e departamentais, planos de negócios;*
- ✓ *Planos de desenvolvimento para TI, outras infraestruturas e edifícios;*
- ✓ *Orçamentos;*
- ✓ *Auditoria externa e consultoria, relatórios de inspeção e revisão;*
- ✓ *Planos operacionais e estratégicos de auditoria existentes.*

☑ *A categorização do universo de auditoria é algo que exige muita reflexão e pode mudar à medida que o processo de planejamento evolui e você considera riscos e oportunidades individuais (Etapa 2, conforme o parágrafo 17).*

Lembre-se de que você apresentará as categorias em sua estratégia de auditoria para que elas façam sentido para os gerentes da organização.

Buscando opiniões dos gerentes seniores

30. Os gerentes seniores devem ser consultados sobre suas opiniões sobre a importância dos sistemas identificados e os controles existentes e o ambiente geral de controle. As discussões com esses gerentes devem ser conduzidas de maneira aberta e com foco em:

- Esclarecer os principais objetivos da organização e o papel dos departamentos individuais na consecução desses objetivos;
- Identificar os principais riscos que eles enfrentam para alcançar os objetivos da organização e seus departamentos;
- Os resultados do trabalho de auditoria interna e externa realizado durante o ano;
- Quaisquer áreas de preocupação que os gerentes possam ter sobre o controle interno ou a eficiência dentro de seu departamento ou nas prioridades da organização para garantia e atenção da auditoria.

Capítulo 3. Identificando riscos e avaliando sua probabilidade e impacto

31. Depois de identificar o universo de auditoria dos objetos auditáveis, a próxima etapa do processo é identificar os riscos específicos. O objetivo é que a AI obtenha um entendimento completo dos riscos que a organização enfrenta e seu potencial impacto e probabilidade, para que esse conhecimento possa ser usado ao pontuar fatores de risco genéricos para selecionar objetos de auditoria para exame (conforme explicado no Capítulo 4).

☑ ***Risco é um termo geral que pode ser difícil de entender***. *No entanto, quase todo mundo entende o que é um evento. Pensar em eventos que podem impactar os objetivos é o caminho mais fácil para identificar riscos*.

☑ ***Similaridades entre categorizar o universo de auditoria e identificar os riscos.***

- ✓ *A identificação dos principais riscos pode sugerir mudanças na maneira como o universo de auditoria é categorizado. Por esse motivo, identificar riscos e categorizar o universo de auditoria pode ser realizado ao mesmo tempo ou de maneira interativa.*
- ✓ *As categorias usadas para o universo de auditoria também podem ser úteis para debater possíveis eventos.*

A boa prática é que a identificação e a avaliação de riscos (pontuação de impacto e probabilidade) sejam realizadas em duas fases. O motivo é que a primeira fase (identificação de riscos) é muito semelhante ao "*brainstorming*", onde o objetivo é capturar todos os riscos. A segunda fase é sobre a aplicação de julgamentos realistas sobre a importância e a probabilidade dos riscos identificados. Pode ser complicado combinar essas duas maneiras diferentes de pensar sobre riscos.

☑ ***Realize a avaliação de riscos em duas fases bem definidas***. *Use a primeira fase para identificar os riscos e a segunda para avaliar (pontuar) os riscos em termos de impacto e probabilidade.*

Identificando eventos que podem dar origem a riscos e oportunidades em todo o universo de auditoria

32. A abordagem para identificar eventos será diferente se a administração já tiver um processo de Gestão de Riscos da entidade que identifique eventos e avalie os riscos.

- Onde houver um processo de gestão de riscos, a AI precisará (a) examinar os registros de riscos para entender os eventos que os gerentes identificaram e depois revisá-los para determinar se a avaliação de riscos identificou todos os principais riscos; (b) revisar a maneira como a administração classificou os eventos e as ações implementadas para lidar com os principais riscos; (c) considerar a eficácia das ações de mitigação de riscos em termos de seu impacto nos riscos residuais; e (d) identificar altos níveis de risco residual que precisam ser levados em consideração nos planos de trabalho estratégicos e anuais.
- Quando não houver processo de gestão de riscos, a AI precisará realizar um exercício separado para identificar eventos que gerem riscos e oportunidades. Isso é mais difícil e demorado do que revisar as próprias avaliações de risco da administração.

É importante que o processo inclua interação com a administração para obter seus pareceres sobre os principais eventos e riscos que afetam a organização. Também será necessário pontuar eventos identificados em termos de probabilidade e impacto para criar uma pontuação geral de risco.

33. O processo de identificação de eventos e pontuação de riscos como parte de um exercício separado é considerado com mais detalhes nas seções a seguir.

Identificando os riscos

34. Mesmo quando a administração não realizou avaliações formais de risco, muitas vezes haverá outras fontes documentais que podem ajudar a unidade de AI a identificar riscos individuais. Essas incluem:

- Planos operacionais para a organização;
- Relatórios anteriores de auditoria interna ou externa;
- Relatório anual da organização;
- Principais revisões de funções ou atividades realizadas pela administração ou por órgãos (por exemplo, missões de revisão do BM ou da UE).

35. O método mais comum de identificação de riscos será por meio de entrevistas e discussões com a administração. Isso sempre deve ser feito, pois os pareceres da administração sobre riscos são muito importantes.

É útil realizar um workshop conjunto de avaliação de riscos com a administração *e isso também pode incluir uma curta sessão de treinamento sobre gestão de riscos. Isso também pode incentivar a administração a desenvolver seus próprios processos de gestão de risco.*

- ✓ *A primeira parte do workshop seria dedicada à identificação de riscos;*
- ✓ *A segunda parte do workshop avaliaria (pontuaria) os riscos identificados para impacto e probabilidade.*

Para identificar riscos, pode ser útil debater os diferentes tipos de eventos que podem gerar riscos para a organização. Um exemplo é fornecido abaixo com os tipos comuns de eventos que geram risco.

Exemplos de tipos de eventos que podem gerar riscos					
Operacional	**TI e Comunicação**	**Regulatório**	**Financeiro**	**Pessoal**	**Reputação**
Perda ou escritórios inacessíveis Indisponibilida-de do pessoal Falhas em utilitário (eletricidade, gás ou água) Sem transporte Falhas críticas de equipamentos / hardware Perda de suprimentos e materIIAs	Perda de internet Perda de telefones Dados indisponíveis ou destruídos Dados corrompidos Ataques virais a softwares-chave Falhas de hardware Registros vitais destruídos ou inacessíveis	Violações de contrato Descumprimento da legislação essencial Multas da UE por não conformidade com regulamentos	Cortes de orçamen-to Perda de subvenção ou financia-mento Roubo ou uso indevido de fundos Falta de caixa para operações	Perda de pessoal-chave (demissão, aposentadoria) Acidentes envolvendo funcionários Falta de integridade dos gerentes Falta de habilidades e qualifica-ções	Publicidade negativa na mídia Níveis de serviço abaixo das expectativas Perda de confiança de partes interessadas devido a deficiências operacionais

Avaliando os riscos em termos de impacto e probabilidade

36. Depois que todos os eventos (riscos) relevantes forem identificados, eles precisam ser avaliados e pontuados. O risco inerente deve ser avaliado em termos de impacto e probabilidade. O impacto define as consequências financeiras ou não-financeiras para a organização, caso ocorra o risco. A probabilidade define as chances de que o risco possa ocorrer. Avaliar o impacto dos riscos é mais complexo do que avaliar a probabilidade, mas ambos são elementos importantes de uma avaliação de riscos.

37. Recomenda-se não classificar os riscos de maneira puramente matemática. É mais prático avaliá-los e pontuá-los de acordo com critérios predeterminados de impacto e probabilidade. As boas práticas geralmente sugerem o uso de três níveis de pontuação, mas isso pode levar a um excesso de pontuação na categoria intermediária. Uma escala de quatro pontos pode, portanto, ser a mais apropriada (principalmente para avaliar o impacto). Não há regra definida aqui. Os auditores podem escolher o sistema de pontuação que acharem mais apropriado. O exemplo abaixo usa quatro categorias e três também podem ser usadas.

Critérios para avaliar o impacto

38. Poderia haver muitos critérios para avaliar o impacto do risco, mas aqueles limitados a quatro ou cinco são considerados os mais importantes. Os seguintes **critérios para avaliar o impacto** são comumente usados e devem ser considerados:
    - Impacto financeiro. As consequências monetárias para a organização caso ocorra o risco.
    - Impacto na reputação. As consequências em relação à reputação da organização, ministro ou mesmo em nível superior, a reputação de todo o país aos olhos de agências de classificação, parceiros internacionais de desenvolvimento, etc..
    - Impacto regulatório. A ocorrência do risco pode resultar em orçamentos ou programas congelados ou até em multas (por exemplo, fundos da UE).
    - Impacto na missão/alcance dos objetivos/operações. Até que ponto a missão da organização pode ser afetada pela ocorrência do risco.
    - Impacto no pessoal. A perda não planejada de pessoas e habilidades importantes pode afetar significativamente a organização.

39. Para cada critério de impacto no risco, o auditor precisa definir o que representaria diferentes níveis de impacto (Muito Alto, Alto, Médio e Baixo). Isso garantirá que os riscos sejam pontuados de maneira comum. O exemplo abaixo fornece conselhos gerais sobre a classificação de três critérios.

Nível (pontuação)	Exemplo de pontuação de critérios de impacto		
	Financeiro	**Pessoal**	**Operações**
Baixo (1)	O impacto financeiro é menor que xxx, xxx.	Perda não planejada de vários funcionários em uma unidade que pode causar alguma interrupção nas operações da unidade.	Perda limitada e mínima de operações. Interrupção de serviço prontamente recuperável.
Médio (2)	Impacto financeiro relevante superior a xxx, xxx mas inferior a xxx, xxx.	Perda não planejada de várias pessoas-chave em uma unidade que causa interrupção significativa nas operações da unidade.	Perda significativa nas operações, mas restrita a um número limitado de serviços/locais da Organização. Interrupção de serviço prontamente recuperável.
Alto (3)	Impacto financeiro relevante superior a xxx, xxx mas inferior a xxx, xxx.	Perda não planejada de várias pessoas-chave que causa impacto significativo nas operações de um ou mais departamentos.	Perda importante nas operações, mas restrita a um número limitado de serviços/locais da Organização. Recuperação lenta de sistemas.
Muito alto (4)	Impacto financeiro material significativo superior a xxx, xxx.	Lesões graves/morte de pessoal.	Ampla incapacidade organizacional para continuar os negócios normais. Perda significativa de operações. Interrupção generalizada do serviço. Recuperação lenta de sistemas.

O Anexo A fornece um exemplo de critérios de impacto de risco usado em uma unidade de AI em uma Agência da ONU.

Critérios para avaliar a probabilidade

40. O auditor precisa considerar a probabilidade de ocorrência de um evento. Por exemplo, um terremoto pode ter um impacto muito alto, mas não ocorre com muita frequência. O impacto da perda de pessoas ou habilidades pode não ser muito alto, mas pode ocorrer com muita frequência. Os critérios para avaliar a probabilidade geralmente são muito semelhantes e os seguintes podem ser considerados como sendo uma opção.

Nível	Critério	Ponto
Raro	Evento extremamente improvável de acontecer	1
Improvável	Evento tem uma possibilidade remota de ocorrência	2
Médio	Evento bastante provável de acontecer em algum momento no futuro	3
Provável	Provavelmente, o evento ocorrerá (dentro de 1 a 2 anos)	4
Esperado	O evento já está ocorrendo ou espera-se que ocorra	5

Pontuação de riscos para impacto e probabilidade

41. Tendo desenvolvido critérios para avaliar o impacto (pontuação) e a probabilidade, estes precisam ser aplicados a todos os riscos identificados. Isso pode ser feito de maneiras diferentes:

    - As planilhas de pontuação podem ser desenvolvidas e usadas por indivíduos para avaliar riscos e, em seguida, os resultados de pontuações individuais combinados para desenvolver uma média em um grupo de pessoas.
    - A pontuação pode ser feita em uma reunião em que cada indivíduo apresenta sua visão e uma pontuação de consenso é acordada.

42. Qualquer que seja o método usado, lembre-se de que as pessoas avaliam os riscos de maneiras diferentes. Algumas pessoas são, por natureza, avessas ao risco, e outras correm riscos. Se uma pessoa avalia um risco como alto e a outra como baixo, o resultado não deve ser simplesmente médio. Um consenso precisa ser alcançado.

Combinando critérios de avaliação em uma matriz de risco

43. É necessário tomar decisões sobre a combinação das pontuações de impacto e probabilidade de risco. Muitas organizações usam uma matriz e concordam previamente que combinações de probabilidade e impacto representam risco baixo, médio, alto e muito alto.

44. Um exemplo de uma matriz típica é mostrado abaixo. Isso precisaria ser modificado para refletir o método real de pontuação de impacto e probabilidade. Também pode ser tomada uma decisão diferente sobre quais combinações classificar como baixa média ou alta.

			PROBABILIDADE				
Raro / Improvável 1 2			Médio	Provável	Frequente / esperado		
			3	4	5		
IMPACTO	Baixo	1	Baixo	Baixo	Baixo	Baixo	Baixo
	Médio	2	Baixo	Baixo	Médio	Médio	Médio
	Alto	3	Baixo	Médio	Médio	Alto	Muito alto
	Muito	4	Médio	Alto	Alto	Muito alto	Muito alto

☑ ***Lembre-se de que o objetivo desta etapa do processo é obter uma boa compreensão dos riscos na organização.***

- ✓ *A auditoria interna deve avaliar apenas os riscos individuais se a administração ainda não estiver fazendo isso.*
- ✓ *A auditoria interna deve incentivar a administração a desenvolver processos eficazes de gestão de riscos da entidade como parte do controle interno.*

Capítulo 4. Construindo planos estratégicos e anuais com base no risco

45. Nesse estágio, o auditor deve ter um bom entendimento dos riscos que podem impactar a organização. Mas qual a importância desses riscos em relação aos diferentes elementos do universo de auditoria? E como esses riscos podem ser refletidos na estratégia de auditoria e no plano de trabalho anual?

46. O objetivo desta etapa do processo é determinar o que precisa ser auditado a partir do universo de auditoria. Identificar os elementos básicos da estratégia de auditoria em termos dos tipos e ciclos de auditorias que precisam ser realizados. É por isso que esse processo também é chamado de *"avaliação das necessidades de auditoria"*.

47. Como é provável que haja um número alto de possíveis objetos de auditoria e um grande número de riscos, a maioria dos auditores usa um conjunto de **"fatores de risco"** genéricos para revisar a importância de cada elemento do universo de auditoria e determinar a prioridade que deve ser conferida a cada objeto auditável. Embora o termo *fatores de risco* seja usado, eles também podem ser descritos como *fatores de seleção*, porque o objetivo dessa etapa do processo é selecionar as auditorias mais apropriadas a realizar.

> ***Pode ser útil pensar em "fatores de risco" como "fatores de seleção"**, pois o objetivo do processo é selecionar quais objetos de auditoria devem ser auditados e com que frequência isso deve ser feito.*

Identificando os fatores de risco

48. A maioria das organizações usa entre cinco e oito fatores de risco. Com menos de cinco, na média, para auditores internos governamentais. Todas as unidades de AI pesquisadas pelo IIA usam o *grau de materialidade financeira* como um dos fatores de risco (Tabela 3).

49. Os fatores de risco mais usados, com comentários explicativos sobre porque são importantes, são:

Materialidade financeira. O volume de atividade financeira coberta por um objeto auditável é um fator de risco essencial. Objetos de auditoria de alto risco que usam uma parte muito pequena do orçamento podem ter menos prioridade para auditoria do que objetos de auditoria de risco médio que lidam com 50% do orçamento.

Complexidade das atividades. Atividades complexas são mais difíceis de fazer bem e, portanto, mais propensas a não atingir seus objetivos, projetos de construção geralmente custam mais do que o planejado e levam mais tempo para serem concluídos.

Ambiente de controle (conforme definido no COSO). O ambiente de controle às vezes é chamado de "Tom do topo". Um ambiente de controle forte é menos suscetível a fraudes e erros. Em um ambiente de controle forte, existem: objetivos claros, papéis e responsabilidades organizacionais, padrões éticos claros de comportamento, acordos fortes de governança e políticas e práticas eficazes de gestão de pessoas. Um ambiente de controle fraco é mais suscetível à fraudes e erros.

Sensibilidade reputacional. Algumas áreas terão um perfil de mídia mais alto, onde os problemas podem gerar um alto nível de risco para a reputação da organização como um todo.

Risco inerente. Áreas de alto risco inerente exigirão processos de controle eficazes para reduzir o risco envolvido. Esses controles importantes devem ser revisados mais regularmente pela AI.

Extensão da mudança. Sabe-se que a mudança gera um risco maior. Por exemplo: a alta rotatividade de funcionários provavelmente reduzirá a eficácia dos controles, pois os funcionários têm menos experiência; reorganização de funções ou mudança de liderança/gerentes-chave também podem gerar incerteza para a equipe, o que limita sua eficácia.

Confiança na gestão. Bons gerentes geralmente resolvem os problemas com mais eficiência e alcançam melhores resultados do que os gerentes ruins e gerentes mais experientes têm mais chances de identificar e lidar com os riscos. As unidades remotas gerenciadas por funcionários de nível inferior podem ter maior risco.

Potencial de fraude. Alguns sistemas e funções são mais propensos a fraudes e corrupção. Por exemplo, altos níveis de recebimento de dinheiro e responsabilidade delegada de aplicar multas.

Sensibilidade política. Alguns assuntos podem ser mais sensíveis à política do que outros e, portanto, atrair mais atenção das partes interessadas.

Tempo desde a última auditoria. Há um fator de dissuasão em todas as auditorias. Mesmo objetos auditáveis com baixo risco devem ser auditados periodicamente. E aqueles que não foram auditados por vários anos podem se tornar de alto risco.

Observe que o risco inerente pode ser um fator de risco genérico. *O trabalho realizado no Capítulo 3 para identificar e pontuar riscos pode ser usado para identificar áreas de alto risco inerente.*

Tabela 3 - Exemplo de boas práticas - fatores de risco comuns usados pelas unidades de AI

Da pesquisa de governo do IIA
As categorizações mais comuns usadas são:
• Grau de materialidade financeira - 100%
• Complexidade de atividades - 94%
• Ambiente de controle - 94%
• Sensibilidade reputacional - 92%
• Risco inerente - 92%
• Extensão da mudança - 89%
• Confiança na gestão - 83%
• Potencial de fraude - 81%
• Tempo desde a última auditoria - 78%
• Volume de transações - 78%
• Grau de automação - 72%

Vide Anexo C para exemplo dos países da PEM PAL.

50. A decisão sobre quais fatores de risco usar é importante e deve incluir pelo menos alguns dos principais fatores de risco usados em geral pelos auditores internos.

☑ ***Mantenha o número de fatores de risco entre 4 e 8.*** *Poucos fatores de risco limitarão a eficácia do exercício, muitos aumentarão o tempo necessário e não produzirão resultados substancialmente melhores. Lembre-se de que você precisa desenvolver critérios para avaliar cada fator e pontuá-los.*

☑ ***Escolha fatores de risco que fazem mais sentido para a organização que você está auditando****. Não utilize apenas a lista acima se houver outros fatores mais relevantes.*

Desenvolvendo critérios para avaliar a importância de cada fator de risco

51. Após a identificação de vários fatores de risco, é prática comum desenvolver um conjunto de critérios que possam ser usados para pontuar e, portanto, classificar a necessidade relativa de auditar cada um dos possíveis objetos de auditoria no universo de auditoria. O desenvolvimento de critérios pode ser relativamente simples ou bastante complexo, mas muitos fatores usarão algum grau de julgamento, portanto, pode ser mais fácil definir apenas a pontuação mais baixa ou mais alta e deixar o restante para julgamento. O exemplo abaixo fornece critérios possíveis para quatro fatores de risco comuns, dos quais três são de natureza crítica (ambiente de controle/vulnerabilidade, sensibilidade e preocupações de gestão).

Exemplo de pontuação de fatores de risco Cada um dos fatores de risco recebe uma classificação de pontos em uma escala de 1 a 5, conforme explicado abaixo.		
Elemento	**Descrição**	**Ponto**
A Materialidade	O sistema responde por menos de 1% do orçamento anual	0
	O sistema responde por 5 a 10% do orçamento anual	2
	O sistema responde por 25-50% do orçamento anual	3
	O sistema responde por pelo menos 75% do orçamento anual	5
B Ambiente/Vulnerabilidade de Controle	Sistema bem controlado com pouco risco de fraude ou erro	0
	Sistema razoavelmente bem controlado com alguns riscos de fraude ou erro	3
	Sistema com histórico de controle deficiente e alto risco de fraude ou erro	5
C Sensibilidade	Perfil externo mínimo para o sistema	0
	Potencial de algum constrangimento externo se o sistema não for eficaz	3
	Relações públicas importantes ou problemas em um sistema ineficaz	5
D Preocupações de gestão	Sistema de baixo perfil em toda a organização que tem pouco impacto na consecução dos objetivos de negócios	0
	Sistema com alto perfil em passado recente, com uma série de preocupações com a gestão por causa de falhas recorrentes	5

Considere adicionar uma ponderação a cada fator de risco para produzir um índice de risco

52. Nem todos os fatores de risco serão igualmente importantes. Portanto, muitas unidades de AI usam algum processo de ponderação dos fatores de risco para dar uma pontuação mais alta aos fatores considerados mais importantes (por exemplo, questões de materialidade ou gestão). Após adicionar um fator de ponderação, que poderia ser desenvolvido em um workshop com a administração, a pontuação dos fatores de risco e a pontuação de ponderação precisam ser multiplicadas para produzir um índice de risco numérico. O índice de risco pode ser usado para identificar objetos de auditoria com prioridade muito alta, alta, média e baixa. O exemplo a seguir mostra como isso se aplicaria no exemplo mostrado para fatores de risco.

Exemplo de fatores de risco de ponderação

Passo 1 Cada um dos fatores de risco recebe uma ponderação usando o julgamento da importância relativa de cada um dos fatores de risco.

Elemento	Ponderação
A Materialidade	3
B Ambiente/Vulnerabilidade de Controle	2
C Sensibilidade	2
D Preocupações de gestão	4

Passo 2 A pontuação do fator e as ponderações são então combinadas em uma fórmula, que pode ser usada para calcular o índice de risco.

Índice de risco = (A x 3) + (B x 2) + (C x 2) + (D x 4)

Passo 3 Cada objeto de auditoria é então classificado como risco muito alto, alto, médio ou baixo, com base em uma pontuação sugerida no índice de risco, por exemplo:

Pontuação do Índice de Risco	Risco / Prioridade
Acima de 45	Muito alto
40-45	Alto
30-40	Médio
Abaixo 30	Baixo

Seria relativamente fácil modificar esse sistema para uso com uma ampla gama de fatores de risco. Mais ou menos fatores de risco exigiriam uma pontuação diferente no índice de risco para categorias muito alta, alta, média e baixa.

Todos os sistemas de pontuação de risco, por definição, produzem números exatos. Isso pode adicionar um falso nível de precisão ao processo de avaliação. É importante reconhecer que muitos fatores de risco são críticos e não se baseiam em valores absolutos. Uma grande exceção é a materialidade, que também é um fator que geralmente será altamente ponderado. (Observação: existem várias maneiras de determinar a materialidade, mas os modelos mais simples geralmente usam uma porcentagem do total de gastos ou receitas.)

☑ ***Certifique-se de que as pontuações e prioridades do índice de risco sejam razoáveis.*** *(a) Calcule a máxima teórica antes de definir as prioridades do índice e (b) esteja preparado para alterar as prioridades do índice se os resultados forem obviamente irrealistas (por exemplo, se toda auditoria for mostrada como alta prioridade).*

Capítulo 5. Escrevendo e atualizando planos estratégicos e anuais

53. Um plano estratégico e anual abrangente da atividade de AI é fundamental para o sucesso da auditoria interna. Tendo identificado e avaliado riscos em todo o universo de auditoria, o próximo passo no processo é desenvolver planos para abordar as áreas de maior importância. O planejamento garante uma abordagem sistemática das atividades de AI e requer conhecimento e competência em uma ampla gama de áreas, como avaliação de riscos e controle interno.

Plano Estratégico

54. O objetivo do plano estratégico é documentar os julgamentos feitos sobre as "necessidades de auditoria" - o julgamento do auditor interno dos sistemas, atividades e programas que devem estar sujeitos à auditoria para fornecer segurança razoável à administração sobre riscos e a eficácia do controle interno. O plano deve conter:

- Objetivos e indicadores de desempenho claramente expressos que a função de AI alcançará nos próximos 2-4 anos, vinculados conforme apropriado à estratégia da organização.
- A metodologia usada para preparar a estratégia e como a unidade de AI avaliou os riscos que impactam os objetivos da organização.
- Como a unidade de AI abordará as áreas de maior importância ao longo de um período de anos. Geralmente, será necessário identificar ciclos de cobertura para diferentes elementos do universo de auditoria. Alguns sistemas e processos podem precisar ser examinados todos os anos. Outros podem precisar ser examinados a cada três a cinco anos e assim por diante.
- Os recursos necessários e disponíveis para atender a essas necessidades e o impacto das restrições de recursos no nível ideal de cobertura da auditoria.
- Uma avaliação interna dos riscos daqueles eventos que podem impactar a consecução dos objetivos da estratégia de auditoria e ações mitigadoras para lidar com esses riscos. (Por exemplo, falta de pessoal; falta de habilidades e treinamento e outras ações necessárias para lidar com esses riscos).
- Planos para a coordenação do trabalho com outras fontes de garantia (por exemplo, auditoria externa).
- A abordagem para acompanhar as recomendações feitas.
- Os objetivos mais altos ou de longo prazo que a função de AI deseja alcançar, mas pode não alcançar a curto prazo.

Um plano estratégico é uma "vitrine" para a auditoria interna – trate de usá-lo bem. *A estratégia é uma oportunidade de apresentar à administração tudo o que uma unidade de AI pode fazer para ajudar a organização a atingir seus objetivos. Pode ser uma maneira útil de gerar suporte.*

Plano anual de auditoria

55. O plano anual de auditoria traduz o plano estratégico nas atribuições de auditoria a serem realizadas no ano em curso. Ele deve definir o objetivo (título e objetivos) e a duração de cada tarefa de auditoria e alocar a equipe e outros recursos de acordo. O plano deve fornecer uma base para o acordo das atribuições a serem realizadas e o prazo de cada tarefa com os gerentes relevantes. Como estes precisam ser direcionados aos recursos orçamentários disponíveis, geralmente é preferível que o plano de auditoria espelhe o período orçamentário.

56. Ao desenvolver o plano anual, o CAI deve considerar várias contribuições para obter um plano de trabalho realista que agregue valor à organização:

- As premissas do plano estratégico de auditoria e se elas ainda são válidas à luz dos resultados da auditoria.
- O último plano anual (se apropriado), levando em consideração as principais conclusões de auditorias anteriores que indicam mudanças de risco.
- Restrições organizacionais e de tempo. (Por exemplo: mudanças na organização departamental; locais que não podem ser alcançados nos meses de inverno; grandes períodos de férias ou fechamento de escritórios - Natal, Páscoa, Verão, implementação de novos sistemas de TI; períodos de alta carga de trabalho).
- Os recursos que devem ser reservados para o trabalho não-planejado futuro (veja abaixo) para evitar reorganizações frequentes do plano anual.
- Programa opcional de auditorias para substituir as missões de auditoria adiadas e/ou um menor volume de trabalho não planejado do que o previsto.

57. Os planos devem ser preparados antes do início do ano. Nem todas as auditorias serão concluídas dentro de um ano de planejamento, portanto, o plano para o próximo ano deve levar em consideração o trabalho que cruza o final do ano.

☑	***Planeje os recursos realmente disponíveis.*** *Embora as posições vazias possam ser preenchidas durante o ano, é recomendável planejar os recursos que você sabe que possui, e não os recursos que você acha que pode ter.*
☑	Permita tempo suficiente para planejar e relatar o trabalho de auditoria concluído.
☑	***Não corra com o planejamento****. Faça algumas suposições sobre derrapagem - dê tempo suficiente para as respostas da administração às recomendações.*

Mantendo os planos atualizados – monitoramento regular de riscos

58. O risco não é um conceito estático. Ele muda com o tempo. Além disso, eventos que realmente acontecem (por exemplo, uma grande redução no orçamento) geram novos riscos para a organização. (Por exemplo, a realização de um grande projeto de capital, que apresentava baixo risco quando os fundos estavam disponíveis, pode ser de alto risco devido a uma revisão do orçamento.)

59. Os auditores devem, portanto, monitorar eventos significativos que ocorrem durante o ano (por exemplo, revisando novos documentos oficIIAs, relatórios externos, cobertura da mídia e mudanças na estrutura jurídica) e o impacto que estes podem ter no plano de auditoria. (Por exemplo, uma mudança de ministro com visões muito diferentes sobre os projetos de maior prioridade no orçamento.)

Revisão Anual do Plano Estratégico

60. O planejamento é um processo dinâmico. Novos sistemas, informações mais atualizadas e outros desenvolvimentos que afetam a organização podem resultar em uma reconsideração da avaliação das necessidades de auditoria. Por esse motivo, a avaliação do risco de auditoria e o plano estratégico de auditoria devem ser revisados anualmente. O plano deve ser completamente reavaliado no final do ciclo.

61. Ao revisar o plano estratégico de auditoria, o CAI deve considerar:
    - Mudanças que ocorreram na organização, suas atividades, objetivos ou ambiente. Isso pode afetar os riscos que enfrenta na consecução de seus objetivos e, consequentemente, o risco relativo de cada sistema auditável.
    - Os resultados das atribuições de AI realizadas no ano anterior podem levar à revisão original da avaliação de risco e prioridade. Isso pode indicar a necessidade de um redirecionamento do esforço de auditoria, por exemplo, revisitar um sistema específico ou examinar um sistema relacionado.
    - Se os orçamentos ainda são adequados e garantirão a entrega de um serviço de AI eficiente.

☑ ***Atualizar avaliação de risco a cada ano***
Normalmente, será necessário atualizar a avaliação formal de riscos a cada ano e revisar a pontuação dos fatores de risco para verificar se a prioridade dos objetos de auditoria mudou durante o ano.

☑ ***Considerar eventos significativos ocorridos durante o ano***
Se houver um evento significativo durante o ano que tenha um grande impacto no risco (por exemplo, um grande corte nos orçamentos), pode ser necessário revisar os critérios de avaliação e seleção de risco imediatamente para determinar se o plano de trabalho anual precisa ser alterado.

Lidando com pedidos adicionais de auditorias durante o ano

62. Nenhum plano é perfeito. As mudanças são inevitáveis e podem surgir por vários motivos:
    - A organização pode ser reorganizada;
    - Novos gerentes seniores podem ter pareceres diferentes sobre a prioridade a ser dada a atividades específicas;
    - Uma grande fraude pode ser detectada identificando níveis mais altos de risco em uma área específica;
    - O ministro pode solicitar uma revisão antecipada dos assuntos que estavam planejados para o futuro na estratégia.

63. O CAI também precisa manter um equilíbrio entre responder positivamente a essas solicitações e a necessidade de que o programa geral de trabalho forneça um nível adequado de garantia em relação aos principais riscos identificados. Para cada solicitação de trabalho *ad hoc*, deve haver uma discussão com os gerentes seniores sobre os benefícios de responder à solicitação e o impacto que isso terá no plano de trabalho anual. Os resultados dessa discussão devem ser documentados.

64. Quando o CAI concorda em realizar uma tarefa não incluída no plano de trabalho anual, o restante do trabalho deve ser reprogramado e um plano de trabalho deve ser revisado e enviado aos gerentes. Como regra geral, o plano anual não deve ser atualizado mais de uma vez por trimestre.

65. Muitas unidades de AI reservam uma proporção de seus recursos para entregar trabalho não-planejado ou *ad hoc*. Isso é algo que o CAI deve considerar ao longo do tempo à medida que obtém experiência com o nível provável de trabalho não-planejado.

☑ Informe os gerentes sobre o impacto de realizar auditorias adicionais durante o ano. Explique claramente o que você não fará se assumir uma nova tarefa.

Anexo A. Exemplo de critérios de avaliação d

risco quanto a impacto

Avaliação de risco: Critérios para o Impacto de Risco (exemplo da unidade de AI da FAO)

Nível (pontuação)	Critérios				
	Realização dos objetivos	Financeiro	Reputação (integridade, responsabilidade)	Pessoal	Operações
Baixo (1)	Falha na entrega de um resultado organizacional.	Impacto financeiro que pode reduzir o fluxo de caixa em menos de US $ 500,000.	Incompetência / má administração ou outro evento que minará a confiança do público em nível local. Curto período de recuperação. Irregularidade grave.	Perda não planejada de vários funcionários em uma unidade que pode causar alguma interrupção nas operações da unidade.	Perda limitada e mínima de operações. Interrupção de serviço prontamente recuperável.
Médio (2)	Falha na entrega de vários resultados organizacionais.	Impacto financeiro essencial que pode reduzir o fluxo de caixa em mais de US $ 500.000 mas menos de US $ 10 milhões.	Incompetência / má administração ou outro evento que minará a confiança do público em nível regional ou um relacionamento-chave. Período de recuperação curto / moderado. Fraude ou corrupção em pequena escala.	Perda não-planejada de várias pessoas-chave em uma unidade que causa interrupção significativa nas operações da unidade.	Perda significativa nas operações, mas restrita a um limitado número de serviços / locais da organização. Interrupção de serviço prontamente recuperável.
Alto (3)	Não cumprimento de um objetivo estratégico.	Impacto financeiro relevante que pode reduzir o fluxo de caixa em mais de US $ 10 milhões, mas menos de US $ 50 milhões.	Incompetência / má administração ou outro evento que minará a confiança do público em um nível internacional / regional ou um relacionamento-chave. Período de recuperação moderado / longo. Fraude e corrupção em larga escala.	Perda não planejada de várias pessoas-chave, o que causa um impacto significativo nas operações de um ou mais departamentos.	Perdas importantes nas operações, mas restritas a um número limitado de serviços / locais da organização. Recuperação lenta de sistemas.

Nível (pontuação)	Critérios				
	Realização dos objetivos	Financeiro	Reputação (integridade, responsabilidade)	Pessoal	Operações
Muito alto (4)	Falha em entregar mais de um objetivo estratégico.	Impacto financeiro material significativo que pode reduzir o fluxo de caixa em mais de US $ 50 milhões.	Incompetência / má administração ou outro evento que destrua a confiança do público em nível internacional ou um relacionamento-chave. Longo período de recuperação. Fraude, corrupção e irregularidades graves no nível da alta administração.	Lesões graves / morte de pessoal.	Ampla incapacidade organizacional para continuar os negócios normais. Perda significativa de operações. Interrupção generalizada do serviço. Recuperação lenta de sistemas.

Avaliação de risco: Critérios para Probabilidade de Risco (exemplo da unidade AI da FAO)

Nível	Critérios	Pontos
Raro	Evento extremamente improvável de acontecer	1
Improvável	Evento tem uma possibilidade remota de ocorrência	2
Médio	Evento bastante provável de acontecer em algum momento no futuro	3
Provável	Provavelmente, o evento ocorrerá (dentro de 1 a 2 anos)	4
Esperado	O evento já está ocorrendo ou espera-se que ocorra	5

Anexo B. Exemplo de pontuação dos fatores de risco

66. Veja a seguir o exemplo de uma metodologia de avaliação de risco para uso no planejamento do trabalho de AI, baseado no Manual de Auditoria Interna do Governo do Reino Unido.

67. Os quatro fatores de risco utilizados são:

- **A Materialidade** (incluindo níveis absolutos de materialidade e quantias de fundos que passam por um sistema)
- **B Ambiente/vulnerabilidade de Controle**
- **C Sensibilidade**
- **D Preocupações de gestão**

68. Cada um dos fatores de risco recebe uma classificação de pontos em uma escala de 1 a 5. A tabela abaixo explica como essas classificações podem ser aplicadas.

Elemento	Descrição	Pontos
A Materialidade	O sistema responde por menos de 1% do orçamento anual	0
	O sistema responde por 5 a 10% do orçamento anual	2
	O sistema responde por 25-50% do orçamento anual	3
	O sistema responde por pelo menos 75% do orçamento anual	5
B Ambiente/Vulnerabilidade de Controle	Sistema bem controlado com pouco risco de fraude ou erro	0
	Sistema razoavelmente bem controlado com alguns riscos de fraude ou erro	3
	Sistema com histórico de controle deficiente e alto risco de fraude ou erro	5
C Sensibilidade	Perfil externo mínimo para o sistema	0
	Potencial de algum constrangimento externo se o sistema não for eficaz	3
	Relações públicas importantes ou problemas legais porque o sistema é ineficaz	5
D Preocupações de gestão	Sistema de baixo perfil em toda a organização que tem pouco impacto na consecução dos objetivos de negócios	0
	Sistema com alto perfil em passado recente, com uma série de preocupações com a gestão devido a falhas recorrentes	5

69. Cada um dos fatores de risco também recebe uma ponderação usando o julgamento da significância relativa de cada um dos fatores. Isso varia entre os diferentes tipos de organização.

70. Um exemplo de ponderação que pode ser aplicada:

Elemento	Ponderação
A Materialidade	3
B Ambiente/Vulnerabilidade de Controle	2
C Sensibilidade	2
D Preocupações de gestão	4

A pontuação do fator e as ponderações são então combinadas em uma fórmula que pode ser usada para calcular o índice de risco. Por exemplo:

Índice de risco = (A x 3) + (B x 2) + (C x 2) + (D x 4)

71. A fórmula é então aplicada a cada sistema para produzir um índice de risco para cada sistema. Cada sistema é então classificado como alto, médio ou baixo, com base na seguinte matriz:

Índice de Risco	**Categoria de risco**
Acima de 49	Alto
30-49	Médio
Abaixo de 30	Baixo

Seria relativamente fácil modificar esse sistema para uso com uma ampla gama de fatores de risco. Mais fatores de risco exigiriam uma pontuação diferente no índice de risco para as categorias alta, média e baixa.

72. Todos os sistemas de pontuação de risco, por definição, produzem números exatos. Isso pode adicionar um ar espúrio de precisão ao processo de avaliação. É importante, no entanto, ter em mente que muitos fatores de risco são críticos e não se baseiam em valores absolutos. Uma exceção importante é a materialidade, que é um fator que sempre deve ser altamente ponderado.

Anexo C. Exemplo de países da IA CoP

A pesquisa foi organizada por iniciativa da IA CoP e foi projetada para coletar informações compatíveis de todos os países representados no Grupo de Trabalho para Avaliação de Risco da IA CoP.

Representantes de 15 países abaixo preencheram o questionário: **Albânia, Armênia, Bósnia e Herzegovina, Bulgária, Croácia, Geórgia, Hungria, República do Quirguistão, Macedônia, Moldávia, Montenegro, Romênia, Rússia, Sérvia e Ucrânia.**

1. Seu país possui metodologia de avaliação de risco para Auditoria Interna (AI)?

Opções:

a. Não

b. Sim, faz parte do manual de auditoria interna publicado pela [*sic*]

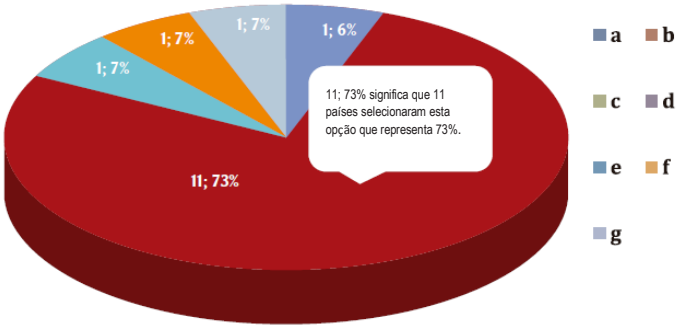
c. Sim, foi publicado pela UCH

d. Ainda não, mas estamos planejando

e. Está em desenvolvimento

f. Cada organização pode desenvolver sua própria AR

g. Outros



- No caso, 11 países fazem parte do Manual de AI, publicado pela UCH.
- Na Ucrânia, cada organização pode desenvolver sua própria metodologia de AR.
- A Geórgia possui o Manual de Gestão de Riscos desenvolvido pela UCH e adotado pelo governo. Estão trabalhando no Manual de AI e a metodologia da AR fará parte disso.
- Na República do Quirguistão, está em desenvolvimento.

2. *Se o seu país possui uma metodologia de avaliação de risco para AI, a mesma é obrigatória?*

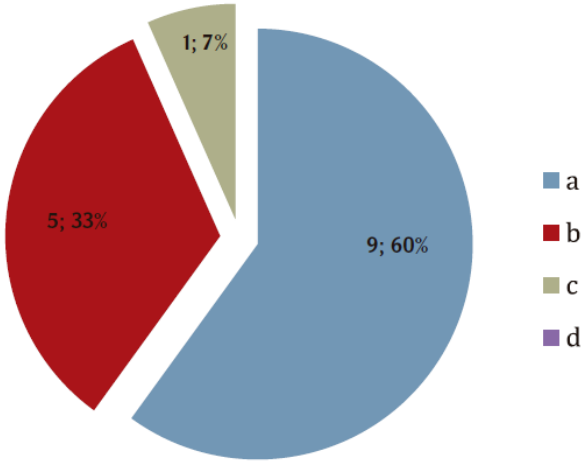
Opções:

a. Sim, toda entidade deve seguir a metodologia

b. Não, é apenas orientação e deve ser adaptada à entidade especificada

c. Não, mas se as unidades de AI tiverem uma metodologia diferente, ela deverá ser aprovada pela UCH

d. Outros

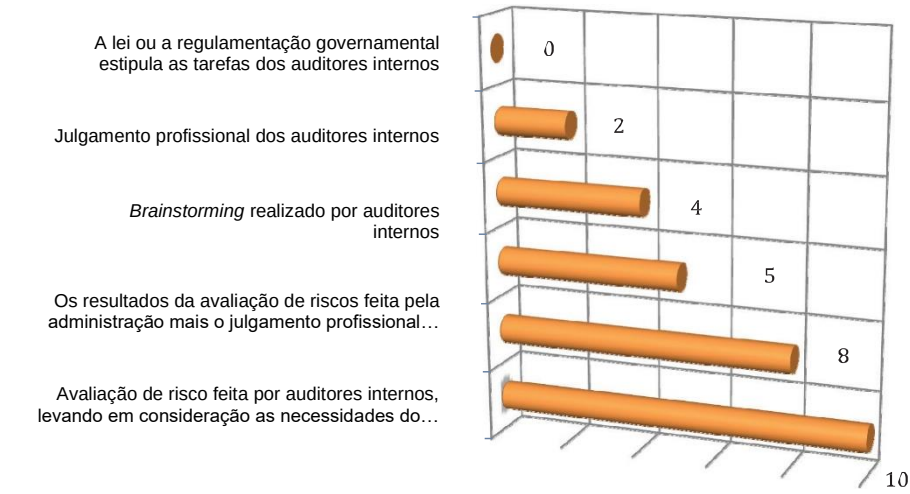


- Em 9 países, é obrigatório.
- Em 5 países, é apenas orientação e deve ser adaptada à entidade especificada.
- No caso de um país, não é obrigatória, mas se uma unidade de AI tiver uma metodologia diferente, deve ser aprovada pela UCH.

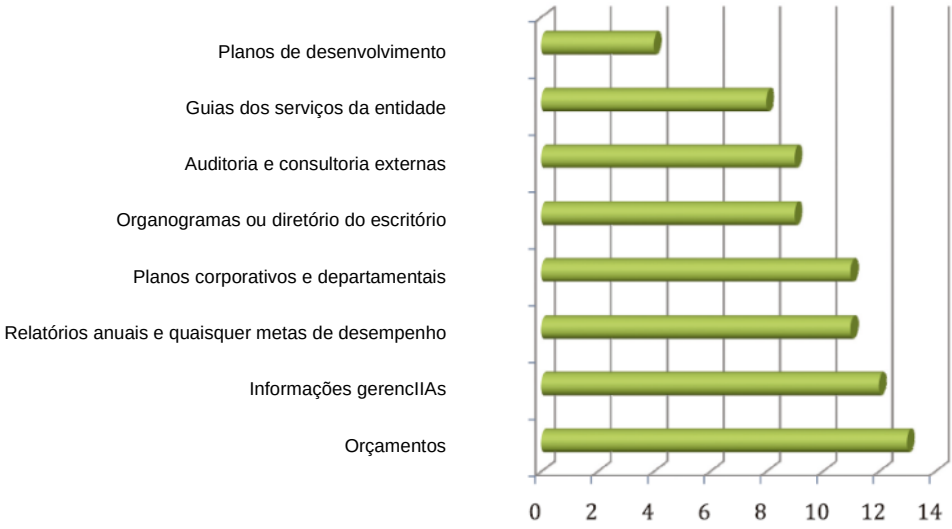
3. *Em seu país, qual é a base do planejamento estratégico da AI?*

Veja as respostas para a questão 4.

4. Em seu país, qual é a base do planejamento anual?6



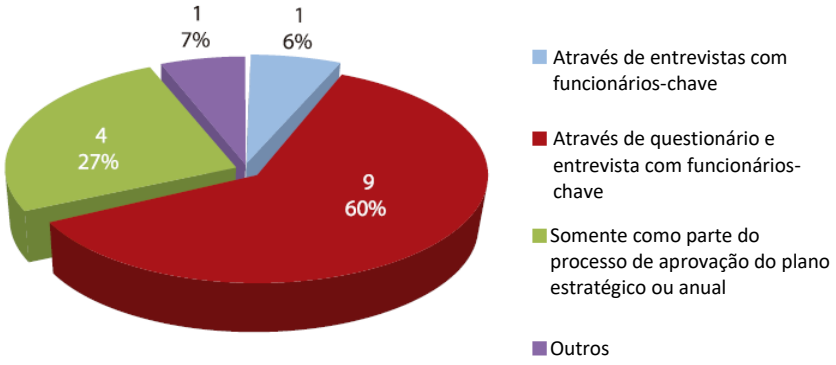
5. Quais fontes de informação são usadas para categorizar o universo de auditoria?



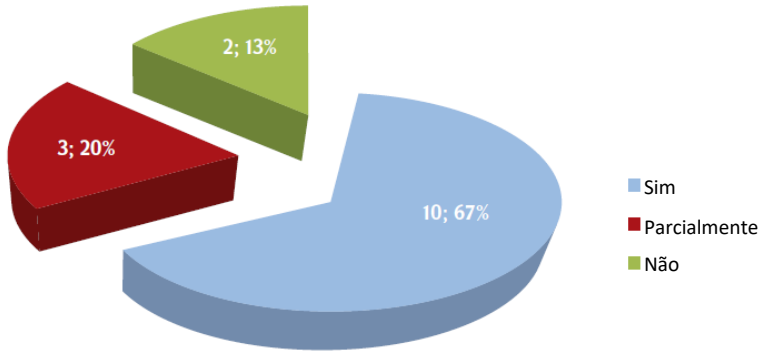
[6] Os textos completos das duas últimas questões são:

- Os resultados da avaliação de riscos realizada pela administração mais o julgamento profissional dos auditores internos
- Avaliação de riscos realizada por auditores internos, considerando as necessidades da administração

6. Como as unidades de AI envolvem os gerentes seniores da organização no planejamento?



7. Todas as unidades de AI têm (ou deveriam ter) um universo de auditoria formalmente documentado?



8. Que categorização do universo de auditoria é usada no seu país?

Opções:

a. Por departamentos
b. Por processos
c. Por unidade organizacional ou local
d. Por programas operacionais
e. Por linhas de serviço
f. Por portfólio de Gestão de Risco
g. Outros

Respostas:

- 7 países usam a categorização por processos, 2 países por unidade organizacional ou local, 1 país por departamentos - por portfólio de Gestão de Riscos.
- A Armênia usa toda a categorização.
- A Bulgária usa uma solução mista: o universo de auditoria pode ser categorizado por departamentos/unidades organizacionais, por processos ou combinação dessas duas abordagens.
- Croácia: pode ser usado todos eles - depende de entidades; principalmente por processos e por programas operacionais.
- A Geórgia usa outra combinação: por departamentos e processos.

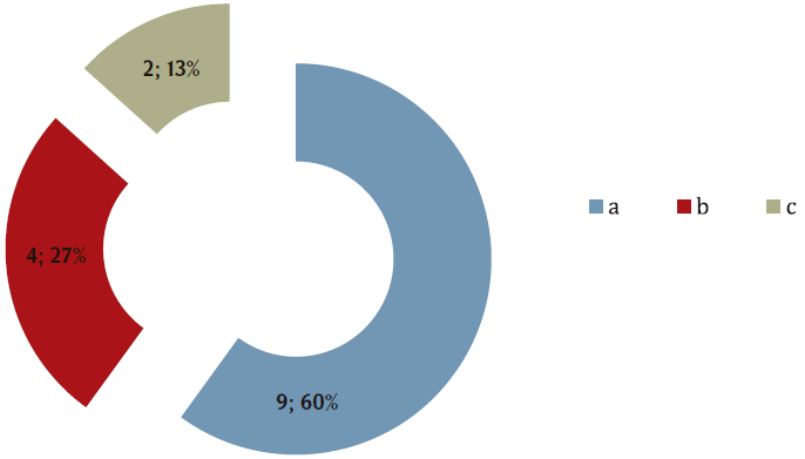
9. *Existe um requisito no seu país para que os gerentes realizem a avaliação de riscos como parte dos procedimentos formais da Gestão de Riscos?*

Opções:

a. Sim

b. Não

c. É necessário, mas poucas organizações realmente têm procedimentos formais de Gestão de Riscos em vigor.



10. A auditoria interna está envolvida na identificação e avaliação de riscos como parte desse processo?

9 de 15 países responderam SIM.

11. Como as unidades de AI identificam riscos?

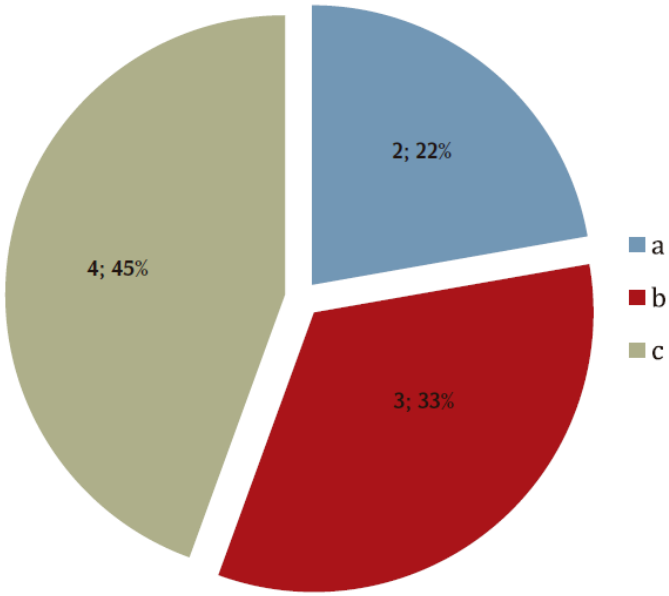
(Esta questão estava vinculada à Q10 - somente os que deveriam responder responderam SIM à Q11.)

Opções:

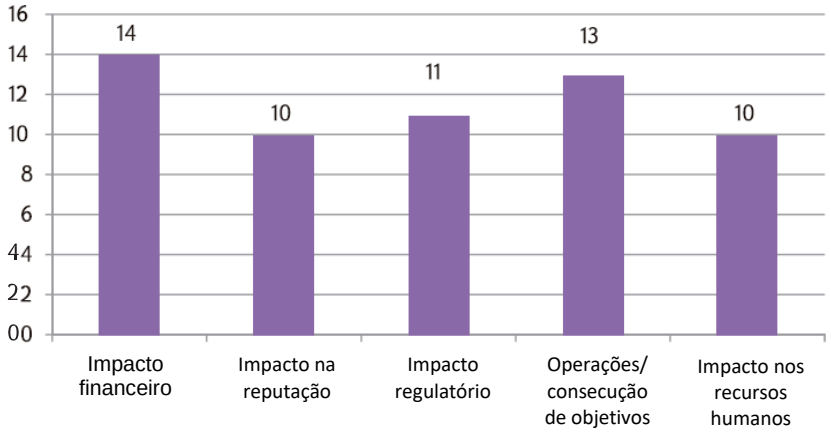
a. Com base no registro de riscos criado como parte do processo de Gestão de Riscos pela administração

b. Dos registros de risco realizados pelos auditores internos

c. No meu país, o método acima mencionado é usado - depende da entidade especificada



12. Quais critérios são usados pela administração ou pela AI para avaliar o impacto dos riscos identificados?



- Bulgária: Os critérios mencionados acima são usados com mais frequência. As diferentes entidades e Unidades de AI podem definir outros critérios relevantes para suas atividades específicas.
- A Croácia usa um tipo adicional: impacto do não alcance das metas estabelecidas.
- Exemplo da Moldávia: Materialidade com uma quota de - 15%; Ambiente de controle - 10%; Sensibilidade -10%; Preocupações de gestão do Ministério das Finanças - 15%; Complexidade do processo -10%; Mudanças de pessoas e de sistema -10%; A integridade do ambiente de processamento de dados - 5%; A última missão de auditoria - 15%; Os resultados da última missão de auditoria - 10%.

13. Como a administração ou a AI classificam o impacto dos riscos identificados?

Veja as respostas na questão 14.

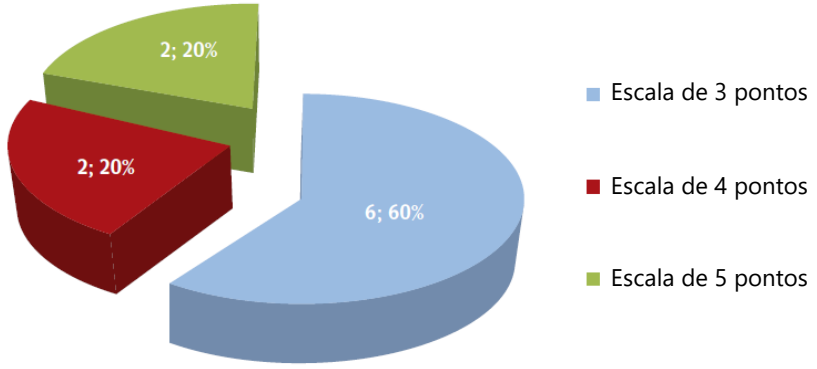
14. Como a administração ou a AI avalia a probabilidade de riscos identificados?

As opções e as respostas foram as mesmas no caso dessas duas questões.

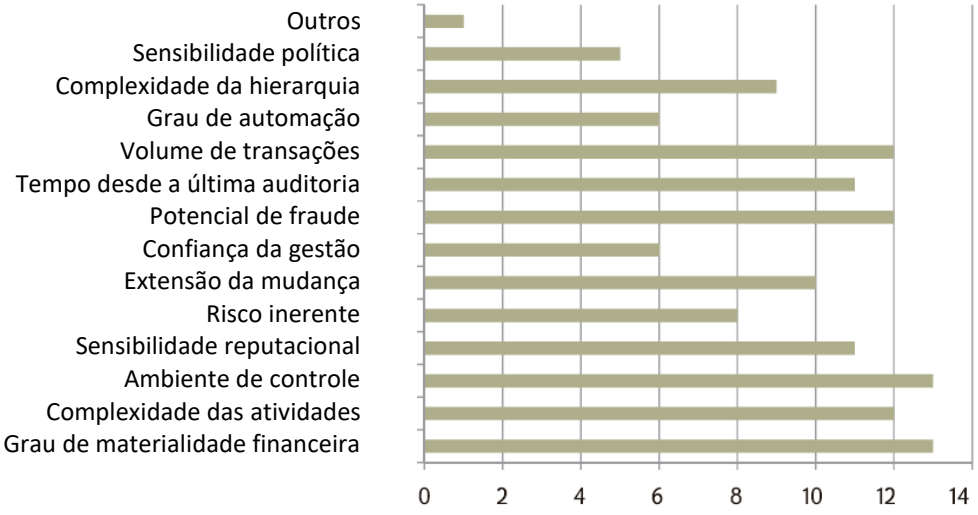
Respostas:

- Bulgária: O modelo da Estratégia de Gestão de Risco para organizações do setor público consiste em uma escala de 5 pontos para avaliação do impacto do risco identificado. Essa escala não é obrigatória - a administração pode escolher a escala de pontos (3/4/5, etc.) que for mais apropriada.

- Geórgia: A IAU está avaliando cada critério/fator de risco com sua pontuação, que é a escala climática de 3 ou 4 pontos; atualmente, a IAU não está usando o modelo de impacto e probabilidade.
- Romênia: todos podem usar uma escala de 3 ou 5 pontos, não é imperativo.

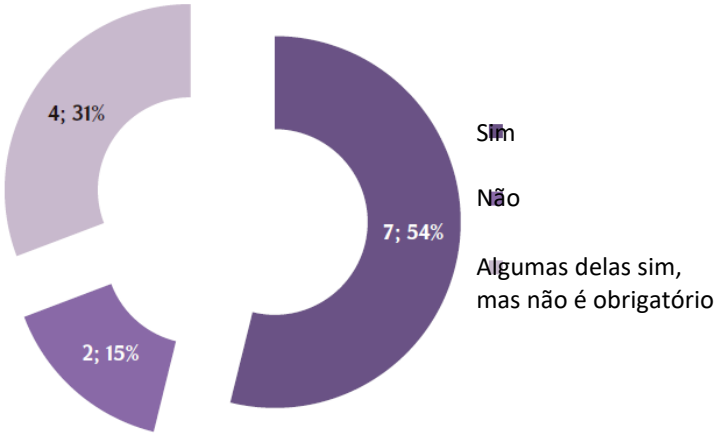


15. Quais fatores de risco genéricos são usados pelas unidades de AI na seleção de elementos do universo de auditoria para exame?

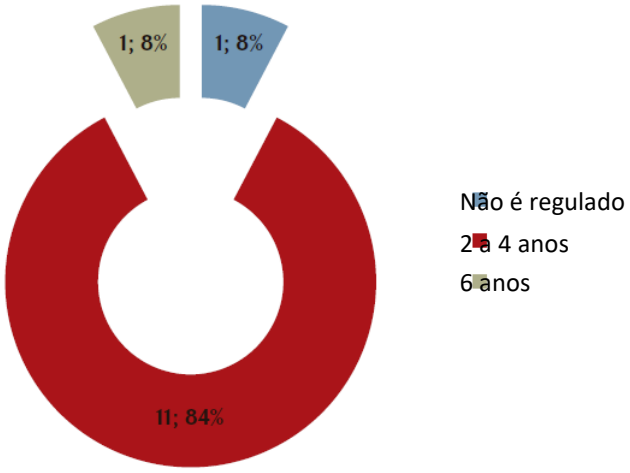


- No caso da Geórgia, também são utilizados os seguintes fatores de risco: Link do sistema com outros sistemas; Tipo e número de processos; Qualificação e experiência dos funcionários; Influência externa; Qualidade e propensão dos controles internos.

16. As unidades de AI acrescentam uma ponderação aos fatores de risco?



17. Que período de tempo o plano estratégico deve abranger em seu país?



Cabe mencionar que 6 países indicaram que o plano estratégico é de 3 anos.

18. Quais das seguintes áreas são cobertas no plano estratégico de auditoria em seu país?

Opções:

a. Objetivos e indicadores de desempenho para a função de AI, vinculados conforme apropriado à estratégia da organização

b. A metodologia usada para preparar a estratégia e como a unidade de AI avaliou riscos que impactam os objetivos da entidade

c. Como a unidade de AI abordará as áreas de maior importância ao longo de um período de anos (ciclos de cobertura para diferentes elementos do universo de auditoria)

d. Os recursos necessários e disponíveis para atender a essas necessidades e o impacto das restrições de recursos no nível ideal de cobertura da auditoria

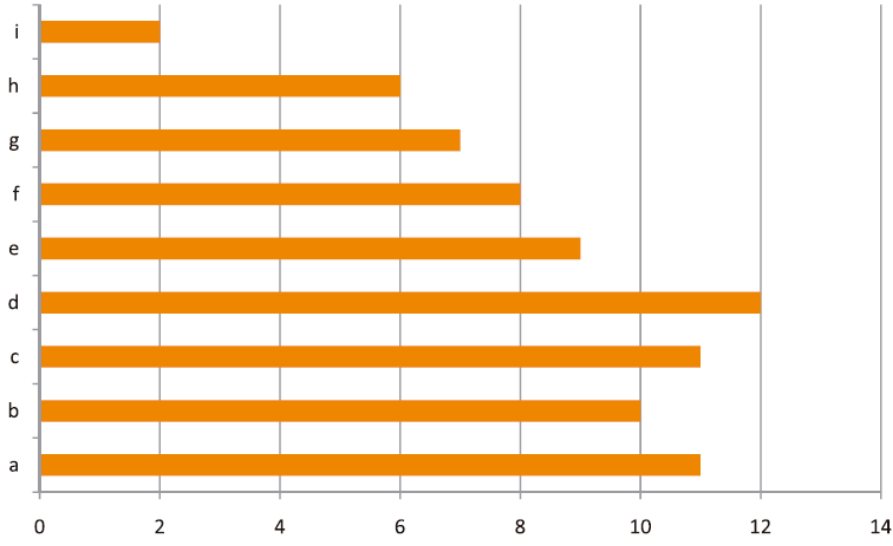
e. Uma avaliação interna dos riscos daqueles eventos que podem impactar a consecução dos objetivos da estratégia de auditoria e ações mitigadoras para lidar com esses riscos (por exemplo, déficit de pessoal; escassez de habilidades e treinamento e outras ações necessárias para lidar com esses riscos).

f. Planos para a coordenação do trabalho com outras fontes de garantia (por exemplo, auditoria externa)

g. A abordagem para acompanhar as recomendações feitas

h. Os objetivos mais altos ou de longo prazo que a função de AI deseja alcançar, mas pode não alcançar a curto prazo

i. Outro(s)



19. *Qual é o conteúdo do plano anual de auditoria em seu país a partir dos seguintes itens?*

Opções:

a. Relação entre os objetivos estratégicos da Unidade de AI e as tarefas planejadas

b. Correspondência entre atribuições planejadas na estratégia de auditoria e no plano anual

c. Objetivo, escopo e duração de cada tarefa de auditoria

d. Objetivo e duração de cada tarefa de consultoria

e. Alocação de pessoal

f. Situação de recursos, incluindo a necessidade de mais recursos, se necessário

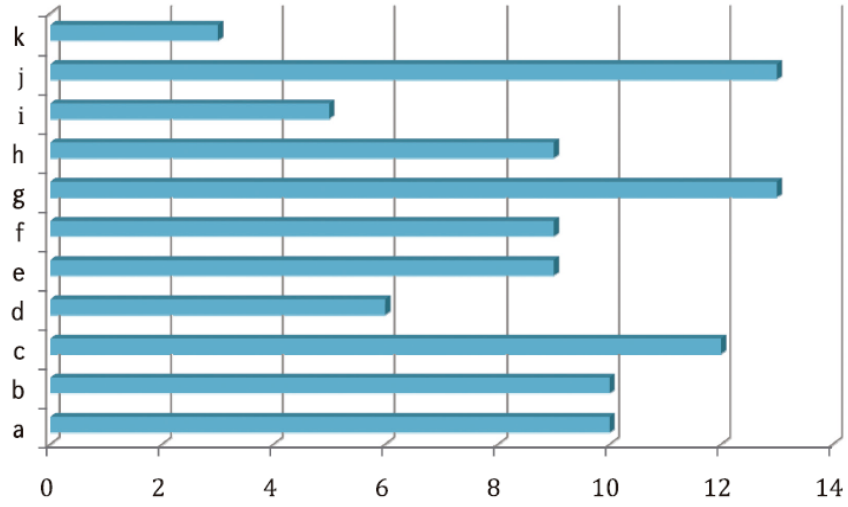
g. Momento das atribuições

h. Plano de treinamento

i. Recursos orçamentários

j. fj. Reserva de tempo para atribuições não planejadas

k. Outro(s)



a. Bósnia e Herzegovina: contém uma seção sobre relatórios, tanto os relatórios anuais regulares sobre o trabalho dos revisores internos da unidade quanto os relatórios periódicos sobre o trabalho da unidade de auditoria interna.

b. Croácia: posição organizacional da Unidade de Auditoria Interna dentro da organização, mudanças na legislação, alocação de funções (quantas auditorias serão realizadas por cada auditor, quantas reuniões, educação, etc.).

C. Geórgia: O plano de treinamento e os recursos orçamentários dependem da IAU; alguns deles podem incluir esse tópico no plano anual.