SÃO PAULO
GOVERNO DO ESTADO

CONTROLADORIA GERAL DO ESTADO

Roteiro para Elaboração de

Plano de Auditoria Interna Baseado em Riscos

SÃO PAULO • JUNHO DE 2023

CONTROLADORIA GERAL DO ESTADO DE SÃO PAULO - CGE

Av. Rangel Pestana, 300 - 18º andar - Sé - CEP: 01017-911
controladoria_geral@sp.gov.br

WAGNER DE CAMPOS ROSÁRIO
Controlador Geral do Estado

ROBERTO CÉSAR DE OLIVEIRA VIEGAS
Controlador Geral do Estado Executivo

DANIEL DA SILVA LIMA
Chefe de Gabinete

SERGIO FREITAS DE ALMEIDA
RONNYE OLIVEIRA SOUSA
Assessoria Técnica

EDUARDO FUKUNAGA
Coordenador de Auditoria

PEDRO FAGUNDES DE OLIVEIRA FILHO
Coordenador de Planejamento Estratégico e Institucional

VALMIR GOMES DIAS
Coordenador de Ouvidoria e Defesa do Usuário do Serviço Público

FABIANA RIBEIRO NOGUEIRA
Coordenadora de Controle Estratégico e Promoção de Integridade

MARIA HELENA BARBIERI MAGANINI
Coordenadora Correcional

CRISTIANE MARQUES DO NASCIMENTO MISSIATO
Coordenadora de Instrução Processual e Cartorária

JOÃO BATISTA PALMA BEOLCHI
Coordenador de Inteligência e Informações Estratégicas

DANIEL DE SOUSA CAMACHO
Coordenador de Tecnologia da Informação

LISTA DE ABREVIATURAS E SIGLAS

AUDIN	Unidade de Auditoria Interna de Entidade da Administração Pública Indireta
CGE	Controladoria Geral do Estado
CGU	Controladoria Geral da União
ISO	*International Organization for Standardization*
IIA	*institute of internal auditors*
MOT	Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental
NBC TA	Normas Brasileiras de Contabilidade Técnicas de Auditoria Independente
PAINT	Plano de Auditoria Interna
RTA	Referencial Técnico de Auditoria
SFC	Secretaria Federal de Controle Interno
TCU	Tribunal de Contas da União
UAIG	Unidade de Auditoria Interna Governamental

Sumário

1. INTRODUÇÃO

Este Roteiro tem por objetivo auxiliar as Unidades de Auditoria Interna Governamental (UAIG), que, no Estado de São Paulo, são a Controladoria Geral do Estado (CGE) e as Unidades de Auditoria Interna da Administração Pública Estadual Indireta (Audin), a elaborarem seus Planos de Auditoria Interna (PAINT).

Além das questões de natureza legal que exigem a atuação das UAIG, os Planos de Auditoria Interna deverão se concentrar em áreas que apresentem elevados riscos, pois isso permitirá direcionar os esforços da CGE e das Audin às questões que estejam mais expostas a ameaças passíveis de afetar o alcance dos objetivos da organização auditada.

Além disso, os PAINT deverão estar em harmonia com os planos estratégicos das Unidades Auditadas, com as expectativas de sua alta administração e com os seus processos de gestão de riscos, quando existirem e forem considerados confiáveis.

No Brasil, essa nova abordagem, baseada em riscos, vem sendo disseminada pela Controladoria-Geral da União (CGU), que exerce importante papel orientador para as Controladorias Estaduais e Municipais e a CGE tem se beneficiado dessa maior experiência da controladoria federal por meio de atividades de capacitação e troca de experiências.

Este Roteiro, por exemplo, é uma adaptação às necessidades do Estado de São Paulo do conteúdo do trabalho elaborado pela CGU denominado "Orientação Prática: Plano de Auditoria Baseado em Riscos", aprovado pela Portaria CGU nº 1.055, de 30 de abril de 2020, à qual a CGE dá os devidos créditos.

Aqui são apresentados conceitos, procedimentos e práticas que, em conjunto, contribuem para que as atividades de Auditoria Interna desenvolvidas pelas UAIG (CGE e Audin) possam agregar valor à gestão estadual, fomentando a melhoria dos processos de governança, de gerenciamento de riscos e de controles internos, mediante abordagem sistemática e disciplinada, baseada em risco[1].

[1] Segundo a norma ISO 31000:2018, "risco é o efeito da incerteza nos objetivos".

2. VISÃO GERAL DO PROCESSO

A expressão “Planejamento de Auditoria Baseado em Riscos” compreende, em termos gerais, as etapas de elaboração do Plano de Auditoria Interna (PAINT), e de planejamento dos trabalhos individuais de auditoria, ambos com base em riscos.

Neste Roteiro, serão abordados apenas os procedimentos relativos à fase de planejamento anual da atividade de auditoria interna, uma vez que as orientações relativas ao planejamento dos trabalhos individuais serão tratadas em norma específica.

O processo de planejamento anual da atividade de auditoria interna se divide em duas etapas: na primeira, são identificados, estudados e priorizados os objetos que compõem o Universo de Auditoria e, na segunda, estabelecem-se quais serão os objetos de auditoria que comporão o PAINT da UAIG (CGE ou Audin) para cada exercício, mediante a consideração de outros fatores, como projetos de execução obrigatória, oportunidade de atuação e questões relativas à capacidade operacional.

Figura 1 – Etapas do planejamento anual da UAIG

Fonte: SFC/CGU

O processo de mapeamento e priorização dos objetos do Universo de Auditoria da UAIG se realiza com base nas seguintes etapas:

Figura 2 – Processo de Planejamento da Unidade de Auditoria Interna Governamental

Fonte: SFC/CGU

A primeira etapa consiste no Entendimento da Unidade Auditada. No entanto, como a atuação da CGE compreende diferentes órgãos e entidades governamentais, bem como as diversas áreas de atuação do Governo Estadual, para os fins deste Roteiro, a primeira etapa do processo de planejamento da UAIG será denominada "**Entendimento do Contexto**", de forma a abranger tanto as instituições públicas (unidades) quanto as áreas de atuação do Governo Estadual. O objetivo dessa etapa é produzir conhecimento e fornecer informações suficientes para possibilitar o desenvolvimento das fases subsequentes.

Na segunda etapa, denominada "**Definição do Universo de Auditoria**", a equipe estabelecerá o conceito a ser aplicado para definição dos objetos de auditoria e, então, identificará os objetos constantes do universo em estudo.

A etapa seguinte consiste na "**Avaliação da Maturidade da Gestão de Riscos**" da Unidade (ou Unidades relacionadas à área de atuação governamental em estudo). Essa avaliação deve possibilitar às UAIG (CGE ou Audin) a tomada de decisão sobre em que medida ela poderá, ou não, valer-se dos riscos que eventualmente já tenham sido mapeados e avaliados pela gestão.

Finalmente, a UAIG deve proceder à "**Seleção dos Trabalhos de Auditoria com Base em Riscos**", utilizando, para tanto, o cadastro de riscos da Unidade Auditada, se confiável, e, se não houver, o mapeamento de riscos realizado pela própria CGE ou Audin ou, ainda, em fatores de riscos (por exemplo: materialidade, relevância, criticidade, risco de imagem, número de denúncias, presença na mídia etc).

Dessa forma, o PAINT deve corresponder a um portfólio de projetos de avaliação, consultoria e/ou apuração a serem realizados sobre objetos constantes do Universo de Auditoria previamente mapeado, considerados os riscos associados e demais fatores de priorização estabelecidos.

2.1 UNIVERSO DE AUDITORIA

Universo de Auditoria é o conjunto de objetos passíveis de serem priorizados para a elaboração do

Plano de Auditoria Interna. Os objetos de auditoria podem ser processos, programas, políticas públicas, unidades de negócio, linhas de produtos ou serviços, sistemas, controles, operações, contas, divisões, funções, procedimentos etc. A definição do Universo de Auditoria deve ser lastreada em prévio entendimento sobre o contexto.

Com o Universo de Auditoria mapeado, a UAIG tem a possibilidade de definir sua estratégia de atuação, a extensão da cobertura de seus exames e as diretrizes para a rotação de ênfase[2] dos objetos de auditoria identificados.

No contexto da atuação da CGE, o Universo de Auditoria compreende o conjunto de Universos de Auditoria das diferentes áreas de atuação do Governo Estadual, bem como dos Órgãos e Entidades do Poder Executivo Estadual. Todavia, esses diferentes Universos de Auditoria coexistem de forma interrelacionada e interdependente, formando uma rede, a qual pode ser analisada sob diferentes perspectivas.

2.2 PAPÉIS E RESPONSABILIDADES

Para que o processo de mapeamento e atualização das informações relativas ao Universo de Auditoria da CGE seja estabelecido e opere de forma adequada, foram definidos papéis e responsabilidades, conforme disposto a seguir.

Diretor

Os diretores dos Departamentos da Coordenadoria de Auditoria da CGE são responsáveis pelo mapeamento do Universo de Auditoria da CGE. A definição das áreas de atuação do governo sob responsabilidade de cada Departamento é estabelecida pelo Controlador Geral. A definição das unidades do governo associadas a cada área de atuação seguirá a mesma regra estabelecida para o monitoramento de recomendações.

Cabe aos diretores dos Departamentos, em suas respectivas áreas de atuação:

a) definir a prioridade dos esforços de mapeamento;
b) autorizar a realização dos projetos de mapeamento; e
c) designar o supervisor (quando necessário) e a equipe de execução dos projetos de mapeamento.

Supervisor

É responsável pelo acompanhamento e revisão geral dos trabalhos de mapeamento, zelando pela qualidade, tempestividade e adequação dos resultados em face dos objetivos estabelecidos.

[2] A rotação de ênfase constitui um rodízio do foco da auditoria entre os objetos que compõem o Universo de Auditoria em determinado período, de modo a evitar a realização de diversos trabalhos de auditoria sobre um mesmo objeto e a não realização de trabalhos sobre outros objetos associados a um menor risco (ver o RTA).

Equipe

A equipe é responsável pela realização dos levantamentos de informações e as análises descritas neste Roteiro.

A adequada definição da equipe é fundamental para o sucesso do processo. Para tanto, é necessário que ela reúna, coletivamente, conhecimento especializado sobre a Unidade ou a área de atuação governamental em estudo e, também, competências técnicas e interpessoais apropriadas, com destaque para habilidades de facilitação e de comunicação.

Assim como na execução dos demais serviços de auditoria interna, é fundamental que, durante todo o trabalho, a equipe mantenha postura ética e profissional adequada, exercendo seu julgamento com o devido zelo e ceticismo profissional.

Nos casos em que a área de atuação governamental ou a Unidade a ser mapeada guarde relação com mais de uma UAIG, é recomendável que essas unidades sejam devidamente envolvidas nos esforços de mapeamento.

3. PROCESSO DE PLANEJAMENTO DA UNIDADE DE AUDITORIA INTERNA GOVERNAMENTAL COM BASE EM RISCOS

Para que a UAIG agregue valor à gestão, ela deve concentrar seus trabalhos nas áreas e atividades cujo alcance dos objetivos pode ser mais fortemente impactado por eventos internos ou externos, ou seja, nas áreas de maior risco.

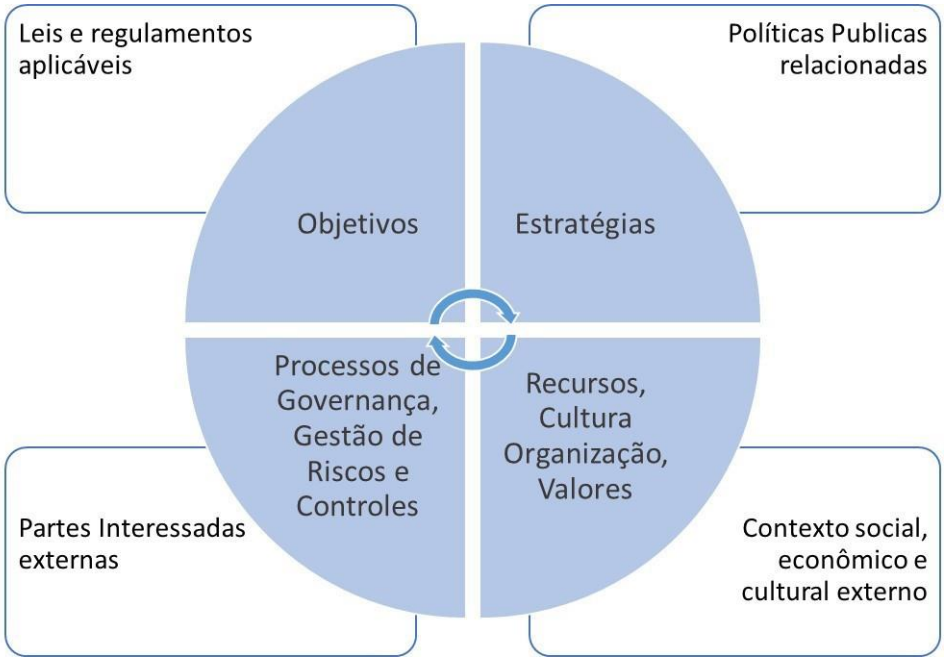
De outra parte, é necessário que haja adequada documentação dos resultados alcançados em cada etapa, bem como sua tempestiva validação junto à gestão, de forma a garantir que o resultado final possa efetivamente corresponder à realidade da Unidade ou da área mapeada.

A seguir são detalhadas as etapas a serem percorridas.

3.1 ENTENDIMENTO DO CONTEXTO

A finalidade dessa etapa é estabelecer o entendimento geral sobre o contexto interno (objetivos, estratégias, processos de governança, gerenciamento de riscos e controles internos, normativos, recursos – humanos, financeiros, tecnológicos etc.) e externo (leis e regulamentos aplicáveis, políticas públicas relacionadas, partes interessadas, ambiente de atuação, indicadores de desempenho etc.), relativos à Unidade ou à área a ser mapeada.

Figura 3 - Entendimento do contexto



Fonte: SFC/CGU

O devido conhecimento do contexto permite a identificação das áreas de maior relevância e dos principais riscos, os quais direcionarão as auditorias que, de fato, agreguem valor e contribuam para o aperfeiçoamento da gestão.

Para tanto, é necessário que a equipe mantenha um ambiente de forte interação e cooperação com as áreas de gestão e partes interessadas envolvidas, de forma a obter as informações necessárias para formar adequadamente seu entendimento. O uso de ferramentas de pesquisa e técnicas de levantamento de informações são particularmente úteis, a exemplo de pesquisas *on-line*, indagação escrita, entrevistas (gestores, servidores, clientes, usuários, beneficiários etc.) e *brainstorming*.

As principais fontes de informação que podem ser consideradas nesse processo[3]são:

a) a alta administração, os gestores dos processos, profissionais com grande conhecimento sobre a Unidade ou área de atuação do Governo e as demais partes interessadas, com quem é possível coletar os dados e elementos pertinentes, bem como suas expectativas em relação à atividade de auditoria interna;
b) áreas responsáveis pelo recebimento de denúncias relacionadas à Unidade ou outras instâncias públicas que detenham essa competência, a fim de subsidiar a elaboração do planejamento;
c) documentos sobre planejamento organizacional (missão, visão, objetivos, valores, metas, indicadores etc.);
d) estrutura organizacional e de governança, e as competências da unidade auditada e suas subunidades;
e) sistemas de gestão empregados;
f) marco legal e regulatório (leis, decretos, regimento interno, regulamentações externas incidentes sobre a Unidade Auditada e suas atividades, bem como políticas, procedimentos e manuais internos relevantes etc.); e
g) resultados de trabalhos de auditoria anteriores.

Com base no conhecimento estabelecido, a equipe deverá documentar as seguintes informações:

Qual é o objetivo da atuação governamental sobre a área estudada ou qual é o motivo de existência da instituição estudada?

Identificar o propósito da existência da instituição ou o papel do Governo Estadual na área de atuação que está sendo estudada. Nesse momento, devem ser identificados a missão e os objetivos-chave, a visão de futuro, os valores fundamentais da organização ou do Governo Estadual na área de atuação em análise.

Como acontece?

Descrever o processo de funcionamento da organização ou da área de atuação do governo, incluindo, no que couber, informações sobre organograma, agentes envolvidos, objetivos estratégicos e os macroprocessos[4] finalísticos e de apoio existentes, entre outras.

[3] Lista adaptada do RTA.

[4] Macroprocesso é o meio pelo qual a organização reúne grandes conjuntos de atividades para gerar valor e cumprir sua missão institucional, de forma alinhada aos seus objetivos. Exemplos: macroprocessos de “Gestão do Controle Interno Governamental” e “Gestão do combate à corrupção“. Cada macroprocesso é composto por diversos processos, a exemplo de “Gerenciar auditorias governamentais”, “Desenvolver

O que faz?

Detalhar o resultado entregue pela organização para cumprimento de seu propósito ou pelo Governo Estadual na área de atuação em estudo, bem como as medidas de desempenho aplicáveis (metas, indicadores e variações aceitáveis no desempenho) e o histórico dos resultados alcançados.

O Anexo I fornece um modelo de documento para apoiar o registro das informações e entendimentos firmados pela equipe sobre o contexto do Universo estudado.

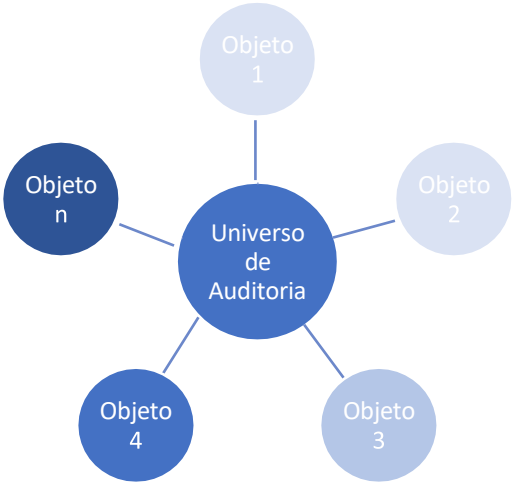
3.2 DEFINIÇÃO DO UNIVERSO DE AUDITORIA

Nessa etapa, a partir do entendimento geral formado sobre a Unidade ou área de atuação do governo será estabelecido o conceito de objeto de auditoria que será adotado e sua posterior aplicação.

Por definição, os processos[5] de negócio representam a atuação cotidiana das instituições e guardam estreita relação com as competências da Unidade ou do Governo Estadual na área em estudo, possuindo certa perenidade organizacional, estando diretamente relacionados com os riscos e com os controles implementados pela organização (o que os torna passíveis de receberem trabalhos de auditoria), sendo, inclusive, mais detalhados do que os macroprocessos finalísticos. Dessa forma, a UAIG deve considerar os processos de negócio (ou grupo de processos correlatos) como o padrão preferencial de conceito para a definição dos objetos de auditoria no contexto do Universo em estudo.

Assim, o Universo de Auditoria será constituído pelo conjunto de objetos mapeados pela equipe sobre os quais a UAIG atuará, por meio de serviços de avaliação, consultoria e/ou apuração, de forma a apoiar o atingimento de seus objetivos, agregar valor, e promover a melhoria dos processos de governança, de gestão de riscos e de controles internos.

Figura 4 – Exemplo de ilustração da composição do Universo de Auditoria



atividades de controladoria" e "Supervisionar órgãos de auditoria interna".

[5] Processo aqui significa um conjunto de atividades sequenciadas e relacionadas entre si que têm como finalidade transformar insumos em produtos e serviços, conforme o MOT.

É necessário que o resultado da definição do Universo de Auditoria seja devidamente documentado, registrando, além da relação dos objetos de auditoria mapeados, uma visão geral sobre cada um dos objetos definidos, incluindo considerações sobre seus objetivos, atividades relacionadas, aspectos organizacionais, marco regulatório, e os arranjos orçamentários, financeiros, de pessoal e de tecnologia da informação existentes, entre outros.

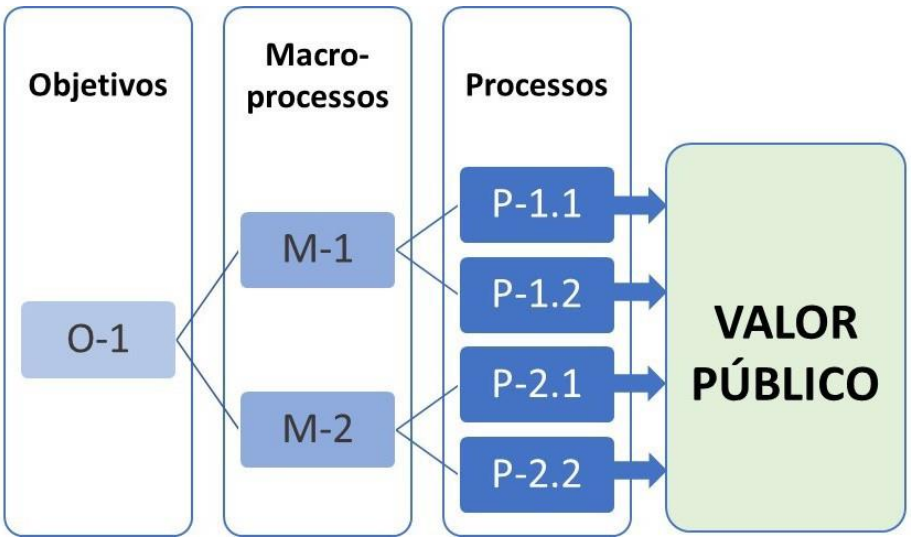
Aspectos relacionados a riscos ou criticidades identificados devem também ser documentados, de maneira a fornecer informações que possam ser consideradas no contexto dos trabalhos individuais de auditoria a serem realizados, além de outros insumos importantes para a posterior priorização dos objetos de auditoria.

A relação completa dos objetos de auditoria identificados no Universo de Auditoria em estudo deve ser devidamente registrada no sistema de gestão da atividade de auditoria. O objeto identificado deve ser cadastrado mesmo que não seja objeto de estudo mais aprofundado no momento do mapeamento do Universo.

O Anexo II apresenta modelo de documento para apoiar o registro das informações e entendimentos da equipe sobre cada um dos objetos de auditoria mapeados.

Seguindo a abordagem sugerida de conceituação dos objetos nos processos, deve-se, a partir do conhecimento dos objetivos (chave e estratégicos), identificar os macroprocessos existentes e, para cada um deles, o conjunto de processos finalísticos e de apoio (os objetos de auditoria), responsáveis pela entrega de valor pela Unidade ou área de atuação governamental em estudo, conforme ilustrado.

Figura 5 – Relação entre Objetivos, Macroprocessos e Processos

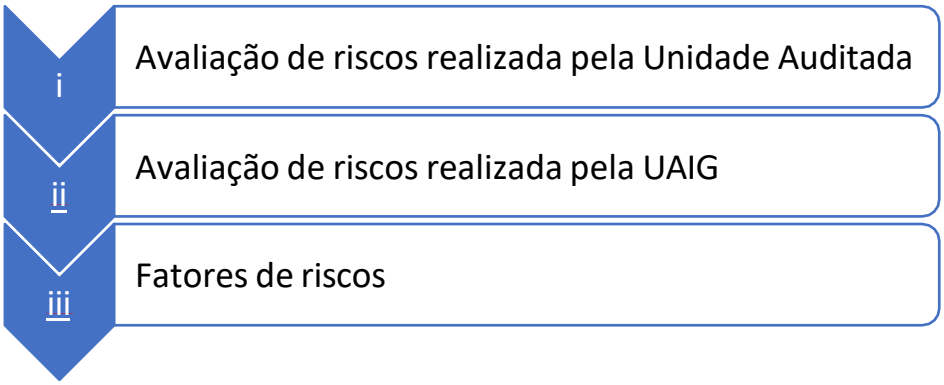


Fonte: SFC/CGU

3.3 AVALIAÇÃO DA MATURIDADE DA GESTÃO DE RISCOS

Existem diferentes bases que podem ser utilizadas para a elaboração do Plano de Auditoria Baseada em Riscos. A seleção da base a ser utilizada deve considerar as condições do contexto e as competências técnicas disponíveis na UAIG.

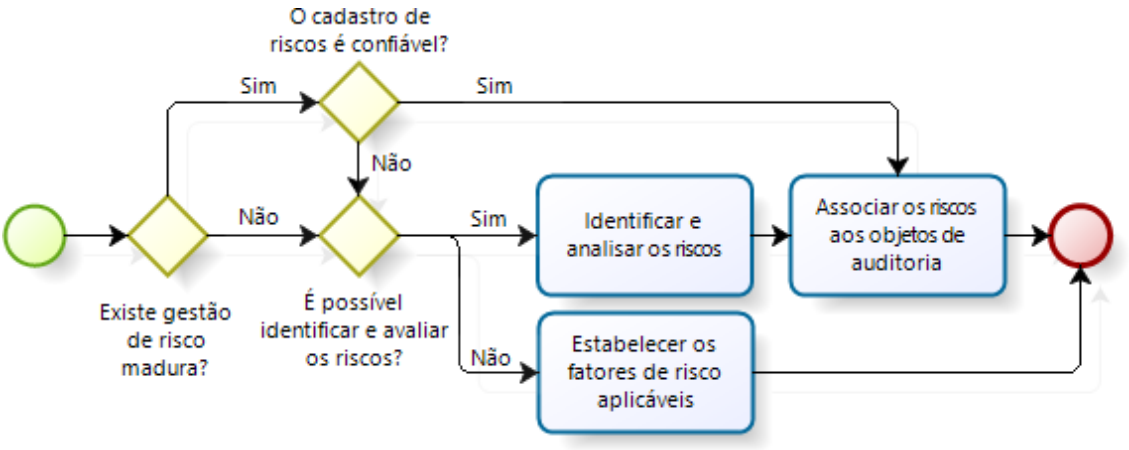
Figura 6 – Bases para seleção dos trabalhos de auditoria



Fonte: MOT

No âmbito da CGE, a elaboração do PAINT deve seguir a ordem acima exposta. Assim, os trabalhos serão priorizados com base em fatores de riscos (exemplos: materialidade, relevância e criticidade) apenas se a avaliação de riscos da própria Unidade Auditada não existir ou não for confiável, e não seja possível ou aplicável a realização de uma avaliação de riscos pela própria UAIG.

Figura 7 – Fluxo de decisões relacionadas com a maturidade da gestão em gestão de riscos



Fonte: SFC/CGU

Dessa forma, o primeiro passo para essa definição é a avaliação da maturidade da gestão de riscos do contexto em estudo. Nos casos em que for considerada madura, deverá servir de referência para a priorização dos objetos de auditoria. Não havendo gestão de riscos madura, é necessário que a própria equipe identifique e analise os riscos do contexto para a posterior priorização de objetos de auditoria.

Para apoiar a avaliação de maturidade da gestão de riscos, é recomendada a utilização do quadro modelo constante no Anexo III deste Roteiro, onde são disposto os quesitos para avaliação. Constatado o nível de maturidade "Aprimorado" ou "Avançado", os riscos mapeados pela gestão devem ser apropriados pela UAIG como variáveis de classificação dos objetos de auditoria definidos.

No caso de não haver maturidade suficiente ou de inexistir gestão de riscos no contexto avaliado, a equipe deve então identificar e avaliar os riscos, de forma a permitir a priorização e a seleção de trabalhos de auditoria sobre objetos que representem maior nível de risco inerente[6].

Ressalta-se não haver expectativa de que esse estudo inicial avance sobre a consideração dos controles implementados e a avaliação dos riscos residuais[7]. No entanto, caso disponível, esse detalhamento fortalece e traz maior assertividade ao processo de priorização que será realizado em seguida.

Por fim, nas situações em que for constatada a inadequação da maturidade da gestão de riscos do contexto e não for aplicável ou viável a identificação e avaliação dos riscos pela UAIG, poderão ser utilizados critérios de escolha, chamados de fatores de riscos, para priorização e seleção dos objetos de auditoria do Universo em estudo.

Em tais casos é necessária a definição prévia dos critérios de priorização a serem utilizados, adaptados ao contexto sob estudo, devidamente validados junto ao supervisor do trabalho de mapeamento do Universo de Auditoria.

3.4 SELEÇÃO DOS OBJETOS DE AUDITORIA COM BASE EM RISCOS

Finalizada a etapa de avaliação da maturidade da gestão de riscos e definida a base a ser utilizada para priorização dos objetos, dá-se início ao processo de seleção dos objetos de auditoria com base em riscos. Esse processo observará procedimentos específicos, a depender da forma de seleção definida pela equipe.

3.5 SELEÇÃO COM BASE NA AVALIAÇÃO DE RISCOS REALIZADA PELA UNIDADE AUDITADA

Como essa forma de priorização se baseia no cadastro de riscos da Unidade Auditada, é possível que não haja uma correspondência direta entre os riscos identificados pela gestão e o Universo de Auditoria mapeado pela equipe.

Nesses casos, será necessário primeiramente realizar a associação entre os objetos de auditoria mapeados e os objetos da gestão de riscos (macroprocessos, processos, unidades de negócio etc.) e, somente então, vincular os riscos (ou conjunto de riscos) aos objetos do Universo de Auditoria.

Na sequência, a UAIG deve classificar os objetos de auditoria com base nos riscos associados a cada

[6] Risco inerente: é o risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.
[7] Risco residual: é o risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

um deles.

3.6 SELEÇÃO COM BASE NA AVALIAÇÃO DE RISCOS REALIZADA PELA UAIG

Para a classificação dos objetos de auditoria, no caso de não haver maturidade suficiente ou em face da inexistência de gestão de riscos na Unidade ou área em estudo, é necessário que a própria UAIG realize a identificação e a avaliação dos principais riscos do negócio.

De forma a equilibrar os aspectos de efetividade, qualidade e viabilidade operacional, foi definido o seguinte modelo padrão[8], a ser aplicado no âmbito da CGE, para priorização dos objetos de auditoria do Universo em estudo com base em riscos:

a) identificação e avaliação dos riscos-chave[9] relacionados aos objetos de auditoria identificados;
b) associação dos riscos dos macroprocessos aos processos (objetos de auditoria); e
c) priorização dos objetos de auditoria com base em riscos.

Como visto anteriormente, nas etapas de entendimento do contexto e de definição do Universo de Auditoria, são identificadas, entre outras informações, os objetivos da Unidade/área em estudo, os macroprocessos e seus respectivos processos (finalísticos e de apoio). Por questões de viabilidade operacional, o modelo preconiza a identificação e avaliação dos riscos apenas no nível dos macroprocessos, com posterior associação aos processos relacionados.

Dessa forma, o primeiro passo consiste na identificação e avaliação dos riscos-chave relacionados aos objetos de auditoria definidos. Para tanto, é recomendado o uso de técnicas como Matriz SWOT, *Brainstorming*, Diagrama *Bow-Tie*, entre outras. A norma ABNT ISO 31010:2009 apresenta e explica o uso dessas e de outras técnicas no contexto dos trabalhos de Gestão de Riscos.

Por exemplo, com a aplicação da Matriz SWOT em cada macroprocesso mapeado é possível identificar forças e fraquezas do ambiente interno e oportunidades e ameaças do ambiente externo ao contexto em avaliação. Com base nas fraquezas e nas ameaças levantadas, podem ser identificados riscos por meio de resposta à questão: "*Quais riscos podem decorrer das fraquezas e das ameaças relacionadas ao macroprocesso?"*.

A partir de então, cada risco identificado deve ser avaliado em relação ao seu potencial impacto (I) e à sua probabilidade (P) de ocorrência, conforme quadro ilustrativo a seguir:

[8] O procedimento padrão foi adaptado do modelo proposto por Santos (2019), considerando que o conceito de objeto de auditoria estabelecido foi por processo. Caso seja estabelecido entendimento diverso, o procedimento deve ser adaptado.
[9] Os riscos-chave são os principais riscos aos quais uma organização está exposta ou o Governo Estadual está exposto em sua atuação na área em estudo.

Quadro 1 – Exemplo de identificação e avaliação de riscos dos macroprocessos

Macroprocessos	Riscos- Chave	Nível de Risco[10] (I x P)
M1. Macroprocesso 1	R1. Risco 1	NR1. 10 x 6 = 60
	R2. Risco 2	NR2. 6 x 6 = 36
	R3. Risco 3	NR3. 6 x 8 = 48
M2. Macroprocesso 2	R1. Risco 1	NR1. 10 x 6 = 60
	R4. Risco 4	NR4. 8 x 8 = 64
	R5. Risco 5	NR5. 8 x 6 = 48
M3. Macroprocesso 3	R4. Risco 4	NR4. 8 x 8 = 64
	R6. Risco 6	NR6. 10 x 4 = 40
	R7. Risco 7	NR7. 6 x 6 = 36
	R8. Risco 8	NR8. 8 x 6 = 48

Fonte: Adaptado de Santos (2019)

O Anexo IV apresenta quadro de apoio ao processo de identificação e análise dos riscos.

O segundo passo consiste na associação dos riscos identificados e avaliados nos macroprocessos a cada um dos seus processos relacionados, que representam os objetos de auditoria mapeados. Essa associação pode ser feita a partir da resposta à seguinte questão, a ser aplicada a cada um dos processos: "*Que riscos relacionados aos objetivos do macroprocesso estão presentes no processo em análise?"* Concluída a associação dos riscos dos macroprocessos a cada um dos processos, é calculada a magnitude dos riscos dos processos, por meio do somatório do nível de risco de cada um dos riscos associados. O quadro a seguir ilustra esse passo:

[10] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação de suas consequências e sua probabilidade (ABNT ISO GUIA 73:2009)

Quadro 2 – Exemplo de associação dos riscos dos macroprocessos aos processos

Macroprocessos	Processos	Riscos Associados	Σ Nível dos Riscos Associados
M1. Macroprocesso 1	P1. Processo 1.1	R1; R2	60 + 36 = **96**
	P2. Processo 1.2	R1; R2; R3	60 + 36 + 48 = **144**
	P3. Processo 1.3	R1; R3	60 + 48 = **108**
	Magnitude do Macroprocesso 1		**348 (24,7%)**
Macroprocessos	**Processos**	**Riscos Associados**	**Σ Nível dos Riscos Associados**
M2. Macroprocesso 2	P4. Processo 2.1	R4; R5	64 + 48 = **112**
	P5. Processo 2.2	R1; R4; R5	60 + 64 + 48 = **172**
	P6. Processo 2.3	R4	**64**
	P7. Processo 2.4	R1; R4	60 + 64 = **124**
	P8. Processo 2.5	R1; R4; R5	60 + 64 + 48 = **172**
	Magnitude do Macroprocesso 2		**644 (45,7%)**
M3. Macroprocesso 3	P9. Processo 3.1	R4; R6	64 + 40 = **104**
	P10. Processo 3.2	R7; R8	36 + 48 = **84**
	P11. Processo 3.3	R4; R6; R7; R8	64 + 40 + 36 + 48 = **188**
	P12. Processo 3.4	R4; R6; R7	64 + 40 + 36 = **140**
	Magnitude do Macroprocesso 3		**416 (29,6%)**

Fonte: Adaptado de Santos (2019)

Por fim, no terceiro passo, a partir da aferição do valor de magnitude dos riscos associados a cada processo, é possível definir a ordem de prioridade dos processos com base em riscos, de forma a subsidiar a elaboração do PAINT.

Quadro 3 – Exemplo de priorização de objetos de auditoria com base em riscos

Prioridade	Processos	Riscos Associados	Σ Nível dos Riscos Associados
1	P11. Processo 3.3	R4; R6; R7; R8	188
2	P5. Processo 2.2	R1; R4; R5	172
3	P8. Processo 2.5	R1; R4; R5	172
4	P2. Processo 1.2	R1; R2; R3	144
5	P12. Processo 3.4	R4; R6; R7	140
6	P7. Processo 2.4	R1; R4	124
7	P4. Processo 2.1	R4; R5	112
8	P3. Processo 1.3	R1; R3	108
9	P9. Processo 3.1	R4; R6	104
10	P1. Processo 1.1	R1; R2	96
11	P10. Processo 3.2	R7; R8	84
12	P6. Processo 2.3	R4	64

Fonte: Adaptado de Santos (2019)

3.7 SELEÇÃO COM BASE EM FATORES DE RISCOS

No caso de se optar pela seleção dos objetos de auditoria com base em fatores de riscos, devem ser definidos os fatores de priorização dos objetos considerando a adequação à realidade da Unidade Auditada e a disponibilidade de dados para aferição dos fatores, sempre com foco nos processos de governança, de gerenciamento de riscos e de controles internos da Unidade Auditada, bem como a possibilidade de ocorrência de erros, fraudes ou não conformidades significativas.[11]

Após a definição e aprovação dos fatores (e eventuais pesos atribuídos) a serem utilizados, a equipe deverá proceder à avaliação de cada um dos objetos com base nos critérios determinados e, a partir de então, promover a hierarquização dos objetos.

Recomenda-se evitar a utilização de fatores que não possam ser associados a todos os objetos de auditoria (a exemplo da materialidade, quando nem todos os objetos possuírem um valor monetário). Caso isso não seja possível, a CGE ou as Audin devem cercar-se de cuidados metodológicos de normalização cabíveis, que permitam a comparação com base nas premissas estabelecidas.

[11] Para mais detalhes e exemplos sobre a definição de fatores de riscos quantitativos e qualitativos, consultar o MOT.

3.8 ELABORAÇÃO DO PLANO DE AUDITORIA INTERNA (PAINT)

Finalmente, no momento de elaboração do PAINT, além da priorização estabelecida no *ranking* acima, a Unidade de Auditoria deverá considerar, por exemplo:

a) a oportunidade de realização de cada trabalho, tendo em vista o contexto político/institucional;
b) a expectativa de agregação de valor e de geração de benefícios financeiros e não financeiros;
c) os trabalhos que devem ser realizados em função de obrigação normativa, por solicitação da Alta Administração ou por outros motivos (decisões judiciais, demandas externas etc.);
d) os trabalhos de auditoria realizados anteriormente sobre o objeto (criticidades e rodízio de ênfase);
e) a disponibilidade dos recursos necessários à realização dos trabalhos; e
f) a capacidade operacional e técnica da UAIG para realizar os trabalhos.

Nesse sentido, os PAINT serão estabelecidos com a inclusão dos objetos de auditoria mais relevantes e oportunos, que possam efetivamente agregar valor à gestão pública.

Importante destacar que, além da relação de trabalhos de auditoria a serem executados no período, devem ser consideradas outras atividades a serem cobertas pelo PAINT, conforme requisitos constantes em normativos específicos, a exemplo de:

a) previsão de, no mínimo, 40 horas de capacitação para cada auditor interno governamental, incluindo o responsável pela UAIG;
b) monitoramento das recomendações emitidas em trabalhos anteriores e ainda não implementadas e em acompanhamento pela UAIG a que se refere o PAINT; ou
c) atividades de gestão e melhoria da qualidade da atividade de auditoria interna governamental.

4. DISPOSIÇÕES GERAIS

4.1 VALIDAÇÃO DOS RESULTADOS COM OS GESTORES

Como forma de assegurar a adequação dos entendimentos e das conclusões dos auditores acerca do Universo de Auditoria, é necessário que tais resultados sejam devidamente validados junto aos responsáveis pela gestão da Unidade ou tema em estudo.

Portanto, é essencial que os trabalhos sejam desenvolvidos com base em um ambiente de colaboração e de interlocução permanente entre as partes, considerando os objetivos mútuos envolvidos e o potencial de agregação de valor à gestão.

4.2 COMPARTILHAMENTO DE INFORMAÇÕES COM OS GESTORES

De acordo com o Instituto dos Auditores Internos, a estrutura de gestão é a:

> "responsável pelo estabelecimento e operação da estrutura de gerenciamento de riscos (...). O papel fundamental do auditor interno em relação ao GRC deveria ser o de prover avaliação (*assurance*) à administração e ao conselho quanto à eficácia do gerenciamento de riscos. Quando a auditoria interna estende suas atividades além deste papel fundamental, deveria aplicar determinadas salvaguardas (...). Desta forma, a auditoria interna irá proteger a sua independência e objetividade dos seus serviços de avaliação (*assurance*). Dentro destas restrições, o GRC (gerenciamento de riscos corporativos) pode auxiliar a ampliar o perfil e aumentar a eficácia da auditoria interna" (IIA, 2009).

Como se pode ver, o processo de gerenciamento de riscos é de responsabilidade da gestão e, portanto, não integra a atividade de Auditoria Interna. Entretanto, em se tratando de unidades com baixo nível de maturidade em gestão de riscos, é esperado que os levantamentos realizados pela auditoria tenham grande valor como fator impulsionador dessa importante atividade de gestão.

Nesse contexto, é oportuno que a identificação e avaliação dos riscos (para fins de seleção dos objetos do Universo de Auditoria) sejam feitas pelo próprio Gestor, com apoio e facilitação realizada pela UAIG, o que permitirá, simultaneamente, a utilização dos resultados pela equipe de mapeamento e o fortalecimento da capacidade da Gestão para gerir seus próprios riscos.

Caso isso não seja possível, visando apoiar a elevação da maturidade em gestão de riscos da Unidade Auditada, a UAIG pode compartilhar os resultados alcançados, desde que adote as devidas salvaguardas. De acordo com o IIA (2009), algumas importantes salvaguardas são:

a) deixar claro que a Administração permanece como a responsável pelo gerenciamento de riscos;
b) a auditoria interna não deve gerenciar nenhum dos riscos em nome da Administração; e

c) a auditoria interna deve dar suporte ao processo de tomada de decisão da Administração, sendo responsabilidade da gestão a tomada de decisões sobre o gerenciamento de riscos.

4.3 PERIODICIDADE DE REAVALIAÇÃO

Esforços de atualização das informações do Universo de Auditoria devem ser realizados, pelo menos, a cada quatro (4) anos.

Todavia, os estudos de entendimento de contextos e de seus riscos devem ser atualizados sempre que ocorrerem mudanças significativas no ambiente que possam comprometer a adequação dos resultados e sua utilidade para fins de definição do Plano Anual de Auditoria Interna.

Mudanças como, por exemplo, modificações no direcionamento estratégico, alterações na política pública, alterações de estrutura organizacional das Unidades envolvidas, novas demandas da sociedade, crises econômicas, entre outras, podem ser indicativos da necessidade de início de um projeto de atualização do Universo de Auditoria.

Importa ressaltar que, após o mapeamento inicial, atualizações tendem a consumir menores esforços e recursos.

4.4 UNIVERSO DE AUDITORIA EM UNIDADES DA ADMINISTRAÇÃO INDIRETA

Pelo fato de as entidades da administração pública indireta do Estado de São Paulo contarem com unidades próprias de auditoria interna, os esforços de mapeamento de Universo de Auditoria da CGE devem ser concentrados, primeiramente, na administração direta e nas áreas de atuação do governo.

Mapeamentos de Universo de Auditoria realizados em entidades da administração indireta devem considerar os conhecimentos gerados pela unidade de auditoria interna atuante na organização. Portanto, caso já existam Universo de Auditoria ou estudos sobre os riscos institucionais e essas informações sejam consideradas maduras e de boa qualidade pela equipe da CGE, devem ser adotados e incorporados ao Universo de Auditoria da CGE.

5 REFERÊNCIAS

- ABNT. **ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário**. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Rio de Janeiro. 2009.

- ABNT. **ISO 31010: Gestão de riscos: Técnicas para o processo de avaliação de risco**. ISO/IEC. [S.l.]. 2012.

- CGU. **Instrução Normativa SFC/CGU nº 3, de 09 de junho de 2017**. Controladoria-Geral da União. Brasília. 2017. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal.

- CGU. **Instrução Normativa SFC/CGU nº 8, de 6 de dezembro de 2017**. Controladoria- Geral da União. Brasília. 2017. Aprova o Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal.

- CGU. **Metodologia de Gestão de Riscos da CGU**. Controladoria-Geral da União. [S.l.]. 2018.

- IIA. **Declaração de Posicionamento do IIA: Declaração de Posicionamento IIA: O Papel da Auditoria Interna no Gerenciamento de Riscos Corporativos**. The Institute of Internal Auditors - IIA. [S.l.]. 2009.

- SANTOS, P. R. M. R. D. **Planejamento de auditoria baseado em riscos: Proposta de aplicação da metodologia de planejamento de auditoria baseada em riscos na seleção de objetos de auditoria relacionados à mobilidade urbana**. Instituto Serzedelo Corrêa. Brasília. 2019. Trabalho de Conclusão de Curso apresentado ao Instituto Serzedello Corrêa como requisito parcial para a obtenção do grau de especialista em Auditoria do Setor Público.

ANEXO I

ENTENDIMENTO DO CONTEXTO

Universo de auditoria estudado (Unidade ou Área de Atuação do Governo):

1. Aspectos gerais da unidade ou da área de atuação do governo

    a) Papel do Governo Estadual na área de atuação;
    b) Objetivos da unidade ou da atuação do Governo Estadual na área;
    c) Missão e visão da(s) unidade(s);
    d) Principais normas (externas e internas) relacionadas à atuação da unidade ou da área de atuação;
    e) Meios pelos quais o desempenho é monitorado;
    f) Política de gestão de riscos vigente no contexto;
    g) Estruturas de governança presentes no contexto.

2. Resultados já alcançados

    a) Políticas públicas relacionadas com o contexto;
    b) Partes interessadas e suas expectativas;
    c) Beneficiários e critérios de seleção;
    d) Resultados alcançados;
    e) Metas, indicadores de desempenho e variações aceitáveis no desempenho;
    f) Histórico dos resultados alcançados;
    g) Boas práticas.

3. Processos e recursos relacionados à Unidade ou Área de Atuação do Governo

    a) Macroprocessos-chave e processos presentes no Universo;
    b) Indicadores de desempenho relacionados ao processo/área auditada, com metas físicas e financeiras;
    c) Responsável(is) pelo objeto (macroprocesso/processo) identificados;
    d) Estrutura organizacional das áreas envolvidas;
    e) Quantidade/lotação/perfil da força de trabalho envolvida (inclusive terceirizados);
    f) Principais insumos utilizados (energia, equipamentos, matéria-prima etc.);
    g) Sistemas informatizados utilizados.

4. Aspectos orçamentários

    a) Programas/ações orçamentários envolvidos;
    b) Materialidade dos recursos (em R$);
    c) Informações por exercício avaliado:
    c.1) Recursos inicialmente solicitados pelo gestor;
    c.2) Execução planejada - físico, financeiro e cronograma;

c.3)Avaliação sumária sobre o planejamento;
c.4) Aspectos operacionais relevantes.

5. Outras informações relevantes

ANEXO II

DOCUMENTAÇÃO DO UNIVERSO DE AUDITORIA

VISÃO GERAL – OBJETO DE AUDITORIA

Universo de auditoria (Unidade ou Área de Atuação Governamental):

Objeto de Auditoria:

a) Descrição do Objeto;
b) Objetivos;
c) Atividades relacionadas;
d) Principais partes relacionadas;
e) Principais arranjos organizacionais existentes;
f) Recursos orçamentários envolvidos;
g) Visão geral sobre estrutura de pessoal existente;
h) Principais sistemas informatizados utilizados;
i) Visão geral sobre o marco regulatório externo vigente; e
j) Visão geral sobre o marco regulatório interno vigente

Obs.: Utilizar 1 formulário para cada objeto de auditoria

ANEXO III

Avaliação de Maturidade da Gestão de Riscos

Universo de Auditoria:

Item de Verificação		Avaliação		Evidências/ Observações
		Nota	Descrição	
Fixação de Objetivos e Metas	A Unidade estabeleceu direcionamento estratégico (objetivos-chave, missão, visão e valores fundamentais) alinhado às suas finalidades e competências legais?	**4**	Avançado	
	A Unidade possui objetivos estratégicos e de negócio claramente definidos e comunicados por toda a organização?	**3**	Aprimorado	
	A Unidade estabeleceu e comunicou adequadamente medidas (metas, indicadores) para monitorar seu desempenho?	**2**	Básico	
	A Unidade estabeleceu o risco aceitável (apetite a risco) para o alcance de seus objetivos?	**1**	Inicial	
Comitê de Governança, Riscos e Controle	A Unidade instituiu Comitê de Governança, Riscos e Controles com competências adequadas?			
	O Comitê tem atuado de forma efetiva na coordenação e supervisão do proceso de gestão de riscos da Unidade?			
Mandato e Comprometimento	A Alta Administração (e as instâncias de governança) demonstram comprometimento e exercem liderança em relação ao processo de gestão de riscos da Unidade?			
	Foi instituída Política de Gestão de Riscos com requisitos mínimos?			
	Foram definidos a metodologia e os critérios para avaliação e documentação dos trabalhos de gerenciamento de riscos?			
	Foi estabelecida estrutura adequada (responsabilidades, pessoas, recursos, ferramentas, informações) para coordenar, implementar e supervisionar o processo de gestão de riscos da Unidade?			
Processo de Gestão de Riscos	O processo de gestão de riscos contém prévia etapa de estabelecimento dos contextos interno e externo onde a Unidade opera de forma a atingir seus objetivos?			
	A etapa de identificação dos riscos fornece informações sobre os riscos			

	relevantes do objeto, incluindo suas causas, eventos e consequências que possam impactar o atingimento dos objetivos?			
	Os riscos identificados são adequadamente analisados em termos de probabilidade de ocorrência e de impacto nos objetivos, de acordo com os critérios previamente estabelecidos?			
	A avaliação e a seleção das respostas aos riscos consideram adequadamente o apetite a risco estabelecido e o custo-benefício das atividades de controle e outras medidas para mitigar os riscos?			
	As respostas aos riscos identificados são efetivamente implementadas?			
	Existe adequado acompanhamento e monitoramento dos riscos e controles-chave pelas áreas responsáveis?			
	O processo de gestão de riscos é adequadamente documentado?			
Resultados	O processo de gestão de riscos está adequadamente implementado em todos os processos operacionais relevantes da Unidade?			
	O resultado da gestão de riscos é oportunamente comunicado à Alta Administração, instâncias de governança e demais partes interessadas?			
	A gestão de riscos tem sido efetivamente utilizada pela Unidade para apoiar o processo de tomada de decisão e a melhoria do atingimento dos objetivos organizacionais?			
	MÉDIA GERAL:	**2,5**	**Aprimorado**	

ANEXO IV

IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS – MACROPROCESSOS

Objetivo-Chave	Macroprocesso	Risco-Chave		Risco Inerente			
		Cód.	Descrição	Impacto	Probabilidade	Nível de Risco	
				5	2	10	Médio
						0	Baixo
						0	Baixo
						0	Baixo
						0	Baixo
						0	Baixo
						0	Baixo
						0	Baixo
						0	Baixo

ASSOCIAÇÃO DE RISCOS AOS OBJETOS DE AUDITORIA

Macroprocesso	Objeto de Auditoria (processos)	Riscos Associados (Código)	Σ Nível dos Riscos Associados

ORIENTAÇÕES

Impacto	Avaliar o impacto do risco com base nos critérios sugeridos na aba "Escalas de Impacto e Probabilidade".
Probabilidade	Avaliar a probabilidade do risco com base nos critérios sugeridos na aba "Escalas de Impacto e Probabilidade".
Risco Inerente (RI)	Risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto. Calculado automaticamente = Impacto x Probabilidade [1 a 100]
Objetos de auditoria	Devem ser listados na aba com o mesmo nome. O Código de cada um deve ser relacionado com o risco na Aba riscos. Ao final devem ser somados os valores das magnitudes dos riscos vinculados

ESCALA DE IMPACTOS		
Magnitude	**Descrição**	**I**
Muito baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, porém causando **impactos mínimos nos objetivos** de prazo, custo, qualidade, escopo, imagem ou relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários).	1
Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos pequenos nos objetivos**.	2
Médio	Interrupção de operações ou atividades de processos, projetos ou programas, causando **impactos significativos nos objetivos, porém recuperáveis.**	5
Alto	Interrupção de operações ou atividades de processos, projetos ou programas da organização, causando **impactos de reversão muito difícil nos objetivos.**	8
Muito alto	Paralisação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos irreversíveis/catastróficos nos objetivos.**	10

Fonte: Brasil. Tribunal de Contas da União. Roteiro de Auditoria de Gestão de Riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017. (adaptada)

ESCALA DE PROBABILIDADES		
Magnitude	**Descrição**	**I**
Muito baixa	**Evento improvável de ocorrer.** Excepcionalmente poderá até ocorrer, porém não há elementos ou informações que indiquem essa possibilidade.	1
Baixa	**Evento raro de ocorrer.** O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade.	2
Média	**Evento possível de ocorrer.** Há elementos e/ou informações que indicam moderadamente essa possibilidade.	5
Alta	**Evento provável de ocorrer.** É esperado que o evento ocorra, pois os elementos e as informações disponíveis indicam de forma consistente essa possibilidade.	8
Muito alta	**Evento praticamente certo de ocorrer.** Inequivocamente o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade.	10

Fonte: Brasil. Tribunal de Contas da União. Roteiro de Auditoria de Gestão de Riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017. (adaptada)