TRIBUNAL DE CONTAS DA UNIÃO

Planejamento de Auditoria com uso de Matriz de Riscos

Arnaldo Ribeiro, CIA, CCSA

Novembro 2016

AGENDA

- ✓Propósito da avaliação de riscos em auditoria
- ✓Modelo de Risco de Auditoria
- ✓Processo de Auditoria Baseada em Risco
- ✓Autoavaliação de Controles (CSA)

Propósito da avaliação de riscos

- **Princípios Fundamentais de Auditoria do Setor Público - ISSAI 100, 40:**
  - é auxiliar o auditor a gerenciar os **riscos de emitir opinião ou relatório** que seja inadequado nas circunstâncias da auditoria.

Sendo aplicável nas Auditorias

- **Financeiras:** é o risco de que o auditor expresse uma conclusão inadequada quando as informações financeiras apresentam distorções relevantes (ISSAI 200, 50)
- **operacionais:** é o risco de obter conclusões incorretas ou incompletas sobre o desempenho, fornecendo informações desequilibradas ou deixando de agregar valor para os usuários (ISSAI 300, 28)
- **conformidade**: o objeto ou a informação do objeto apresentam distorções relevantes de conformidade em relação às normas aplicáveis, o auditor deixa de modificar sua opinião ou abordá-las em seu relatório (ISSAI 400, 46 e 54)

E as normas, o que dizem?

Normas de Auditoria do TCU

Identificação e avaliação de objetivos, riscos e controles

- 71. Para determinar a extensão e o alcance da auditoria que será proposta, a unidade técnica deve dispor de informações relativas aos objetivos relacionados ao objeto que será auditado e aos riscos relevantes associados a esses objetivos, bem como à confiabilidade dos controles adotados para tratar esses riscos...
- 71.1. Alternativamente, caso a auditoria seja proposta sem que as informações relativas aos objetivos, riscos e controles do objeto auditado estejam disponíveis, tais informações deverão ser obtidas na fase de planejamento do trabalho...

E as normas, o que dizem?

IPPF

- 2210 – Objetivos do Trabalho de Auditoria
  - 2210.A1 – Os auditores internos **devem conduzir uma avaliação preliminar dos riscos relevantes para a atividade sob revisão**. Os objetivos do trabalho de auditoria devem refletir os resultados desta avaliação.

- 2201– Considerações sobre o Planejamento

No planejamento dos trabalhos de auditoria, os auditores internos devem considerar:

- ...
- Os **riscos significativos** para os objetivos, recursos e operações da atividade e os meios pelos quais o impacto potencial dos riscos é mantido em um nível aceitável.

E as normas, o que dizem?

Definição de Auditoria Interna

"A auditoria interna é uma atividade **independente e objetiva** de avaliação (*assurance*) e de consultoria, desenhada para **adicionar valor** e melhorar as operações de uma organização.

Ela auxilia uma organização a realizar seus objetivos a partir da aplicação de uma **abordagem sistemática e disciplinada** para avaliar e melhorar a eficácia dos processos de **gerenciamento de riscos, controle e governança**."

Abordagem da auditoria na gestão de riscos

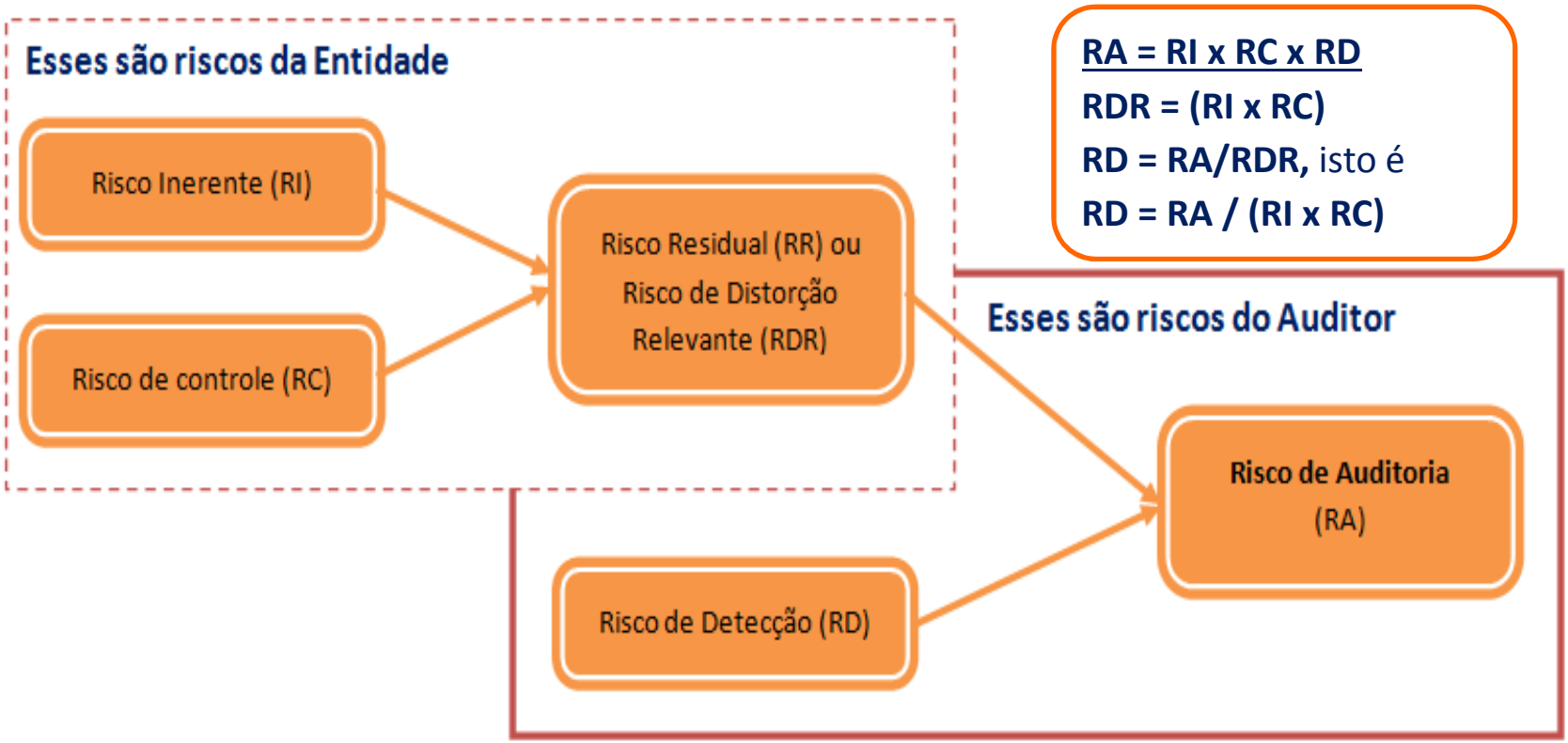
Maturidade	Características da Gestão de Riscos	Abordagem da Auditoria Interna
Ingênuo	Nenhuma abordagem formal	• Promover a Gestão de Riscos • Utilizar a avaliação de riscos feita pela própria auditoria
Consciente	Abo m dispersa e	Promover abordagem formal • Utilizar eita pela própria
	ca e processo efinido	• Facilitar • Utilizar ta pela gestão, onde ap
	s totalmente implementada	• Ut a gestão, onde
	s e Controle Interno totalmente erações	• Auditar Ge e SCI • Utilizar avalia co feita pela gestão

IIA 2009, Norma 2120 - 1, 3 - *"Em situações em que a organização não tenha processos formais de gestão de risco, o responsável pela auditoria precisa discutir formalmente com a administração e com o conselho as suas obrigações de entender, gerenciar e monitor o riscos da organização..."*

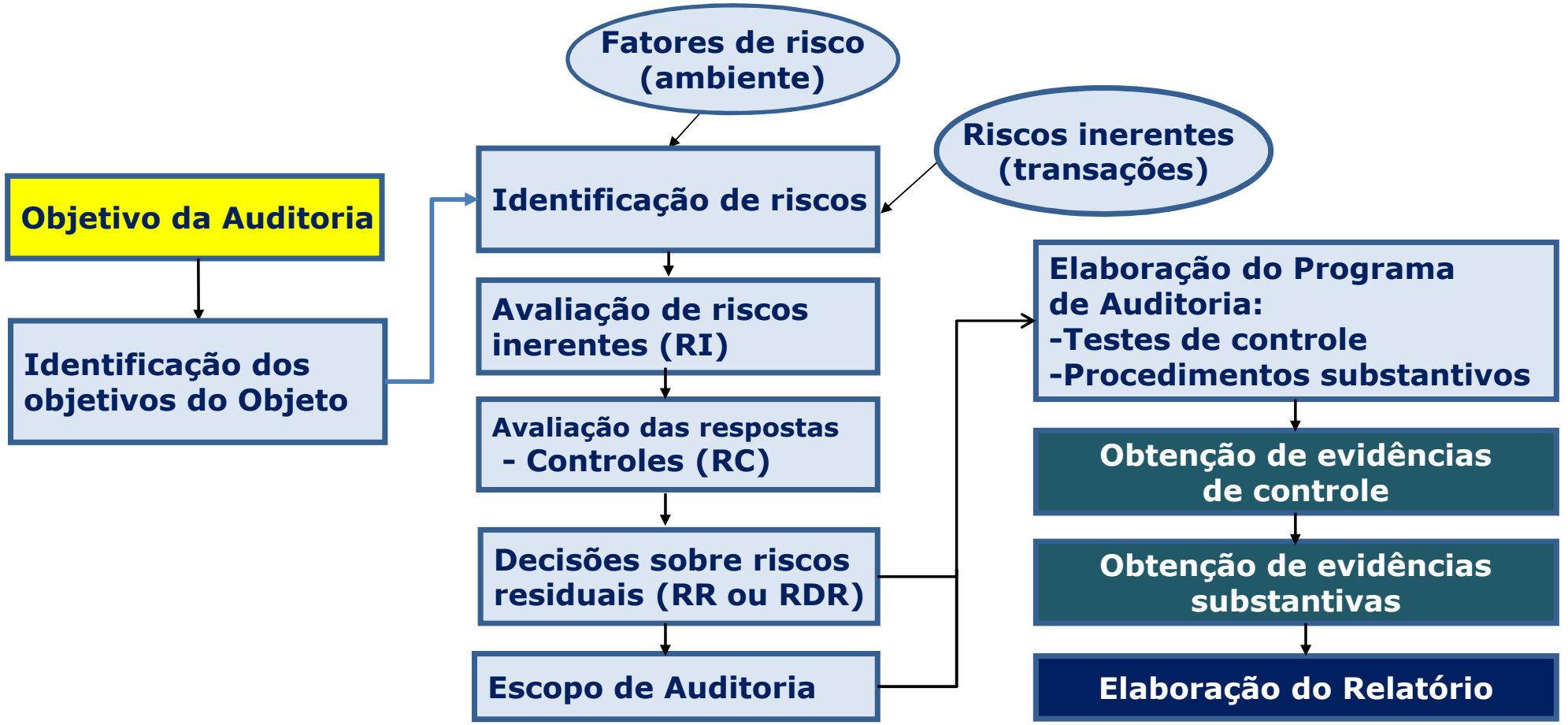
Maior intervenção e envolvimento direto inicial no programa de gestão de riscos

Nenhuma intervenção. Volta ao seu papel tradicional de avaliação e asseguração dos processos integrados de ERM e SCI

O Modelo de Risco em Auditoria



Processo de Auditoria Baseada em Risco



Entendimento do objeto e do seu ambiente

Incluir no planejamento da auditoria **procedimentos preliminares de avaliação de risco**, mediante **entendimento do objeto e do seu ambiente, inclusive do controle interno**, destinada a:

- **Levantar informações preliminares**
  - Pesquisar/requisitar informações ou documentos que as contêm, para entender o negócio e o contexto das operações.
  - Missão, visão, Objetivos estratégicos, táticos, operacionais
  - Trabalhos anteriores, base normativa
  - Análise SWOT, DVR, Ishikawa, etc.

Entendimento do objeto e do seu ambiente

- **Realizar procedimentos analíticos preliminares**
  - Desenvolver expectativas por meio de análises quantitativas de informações históricas de atividades, resultados, indicadores, orçamento e outras.
- **Indagar à administração e a outros (5W2H)**
  - Desenvolver percepções em relação à atividade que será auditada (objetivos, riscos, aspectos de relevância).
- **Observar e inspecionar operações e atividades**
- Entender como as operações e as atividades são executadas e controladas.

Documentação do entendimento

- Convém que um **Memorando Descritivo** seja elaborado para descrever os elementos do processo referenciar os demais documentos utilizados para registrar o entendimento do objeto:
  - ✓**Mapa de Processo** ou **Fluxograma**
  - ✓**Matriz SWOT** e **DVR**
  - ✓**QACI**, se aplicado, e resumo avaliativo do controle interno
- Na fase de relatório o memorando descritivo, revisado após a fase de execução, comporá a seção **Visão Geral do Objeto** do relatório da auditoria.

Elaboração da Matriz de Avaliação de Riscos

1. Identificação dos riscos inerentes
2. Análise dos riscos inerentes (RI = I x P)
3. Identificação dos controles que mitigam os riscos inerentes
4. Avaliação do desenho e da implementação dos controles internos
5. Definição da abordagem de auditoria

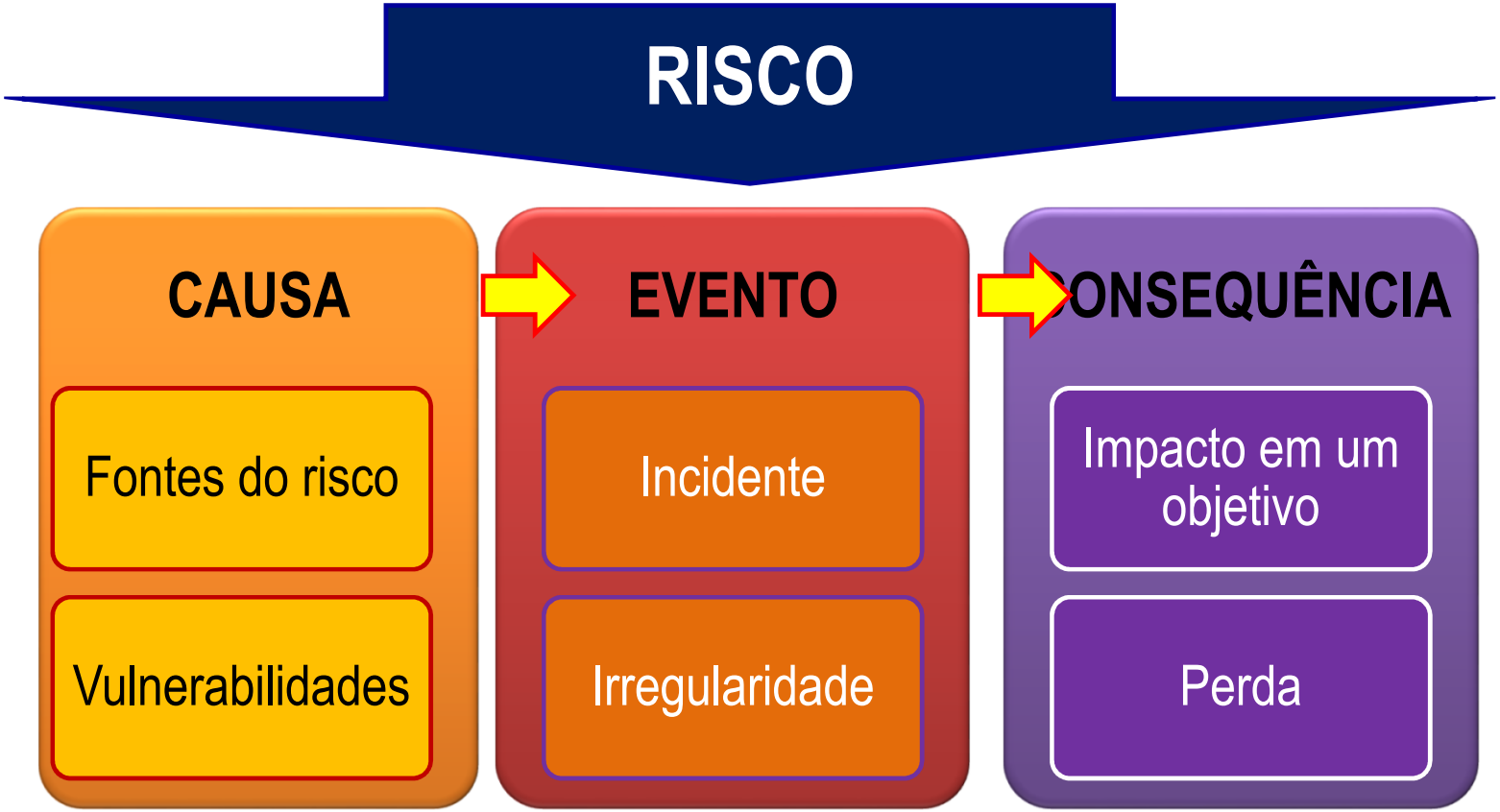
Matriz de Avaliação de Riscos

6. Elaboração e aprovação do Programa de Trabalho
7. Fase Execução
8. Fase Relatório

Identificação dos riscos inerentes

Matriz de Avaliação do Riscos

Componentes do risco



Norma ISO 31000: 2009, item 2.15

Causa = fonte + vulnerabilidade

- **Fonte de risco:** elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco:
  - Pessoas
  - Processos
  - Sistemas
  - Infraestrutura física/organizacional
  - Tecnologia [de produto ou de produção]
  - Eventos externos (não gerenciáveis)
- **Vulnerabilidade:** inexistência/falta, inadequação, insuficiência associada a uma fonte de risco.

Exemplos de Causas

Da Fonte

- **Pessoas**

Vulnerabilidades

- Em número insuficiente
- Sem capacitação
- Perfil inadequado
- Desmotivadas
- ...

Sintaxe para descrição do risco

Devido a <CAUSA ou FATOR DE RISCO = Fonte + Vulnerabilidade>, poderá acontecer <EVENTO>, o que poderá levar a <CONSEQUÊNCIA> impactando no/na <DIMENSÃO DE OBJETIVO>.

Os componentes do risco também podem ser descritos em colunas separadas de planilhas ou registros de bancos de dados.

Evento	Causa	Consequência/Impacto

Avaliação dos riscos inerentes

Matriz de Avaliação de Riscos

Matriz Impacto x Probabilidade

Legenda Nível de Risco Extremo Alto Médio Baixo		Probabilidade				
		1 Muito Baixa	2 Baixa	5 Média	8 Alta	10 Muito Alta
Impacto	10 Muito Alto	10	20	50	80	100 Extremo
	8 Alto	8	16	40	Alto 64	80
	5 Médio	5	10	Médio 25	40	50
	2 Baixo	2	4	10	16	20
	1 Muito Baixo	1 Baixo	2	5	8	10

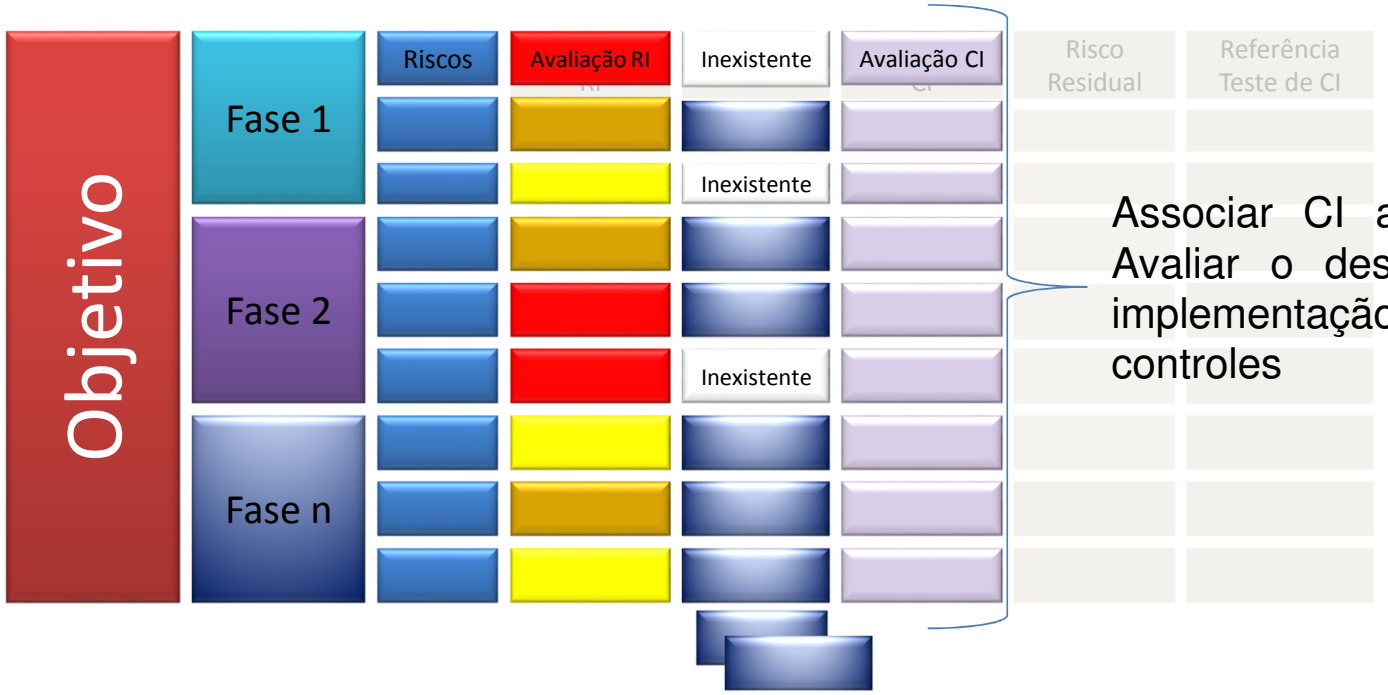
Escala de Probabilidades

Exemplo Qualitativo

Magnitude	Descrição	P
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

Identificação e avaliação das respostas aos riscos inerentes

Matriz de Avaliação de Riscos



Escala para avaliação de desenho e implementação dos controles

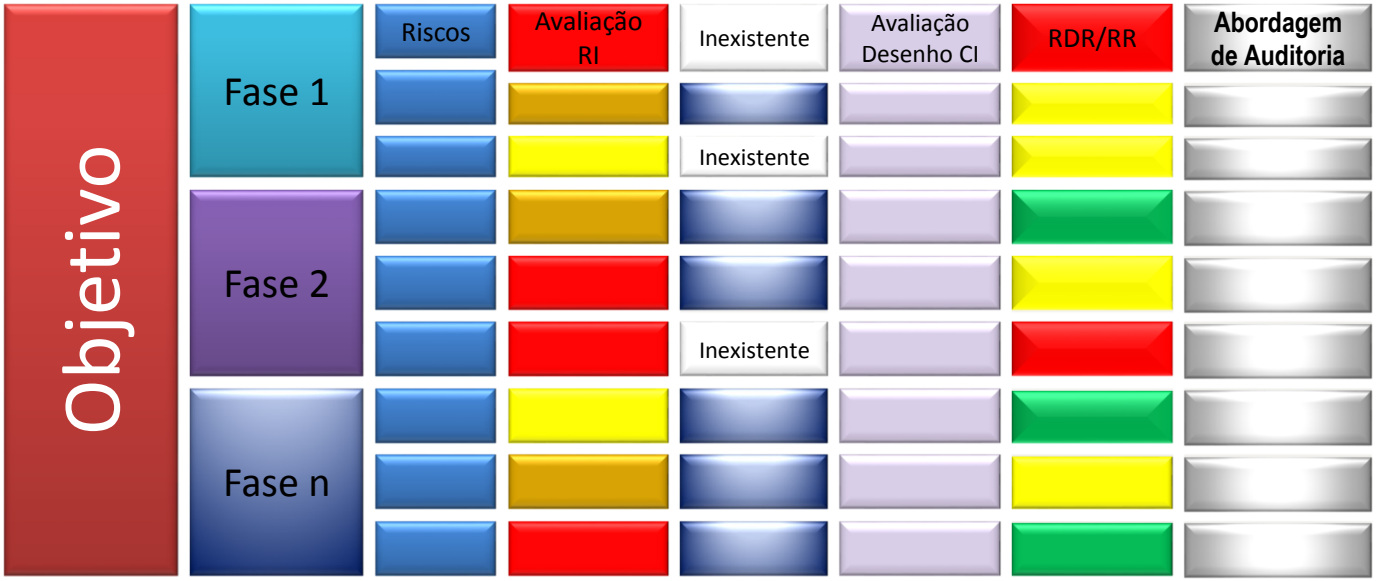
Situação do controle existente	Avaliação do Controle
Controle inexistente ou não funcional/não implementado.	**1 - Inexistente**
Controle não institucionalizado, depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual.	**2 - Fraco**
Controle razoavelmente institucionalizado, mas pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	**3 - Mediano**
Controle institucionalizado e embora passível de aperfeiçoamento, é sustentado por ferramentas adequadas e mitiga o risco razoavelmente.	**4 - Satisfatório**
Controle institucionalizado e sustentado por ferramentas adequadas, podendo ser considerado em um nível de “melhor prática”; mitiga o risco em todos os aspectos relevantes.	**5 - Forte**

Nível de Confiança e Risco de Controle

Avaliação do Controle	Nível de confiança nos controles	Risco de Controle (multiplica o RI)
1 - Inexistente	**Nenhum nível de confiança.** Considerando o Risco Inerente Extremo 100 , o nível de confiança nos controles seria "zero" temos: 100 – 0.	**100**
2 - Fraco	**Nível de confiança de 20%.** O controles são capazes de mitigar 20% dos eventos. Risco de controle = 100 – 20.	**80**
3 - Mediano	**Nível de confiança de 40%.** O controles são capazes de mitigar 40% dos eventos. Risco de controle = 100 – 40.	**60**
4 - Satisfatório	**Nível de confiança de 60%.** O controles são capazes de mitigar 60% dos eventos. Risco de controle = 1 00 - 60.	**40**
5 - Forte	**Nível de confiança de 80%.** O controles são capazes de mitigar 80% dos eventos. Risco de controle = 100 - 80. Pois, devido às limitações inerentes aos controles, eles nunca dão uma garantia absoluta.	**20**

Avaliação dos Riscos residuais

Matriz de Avaliação de Riscos



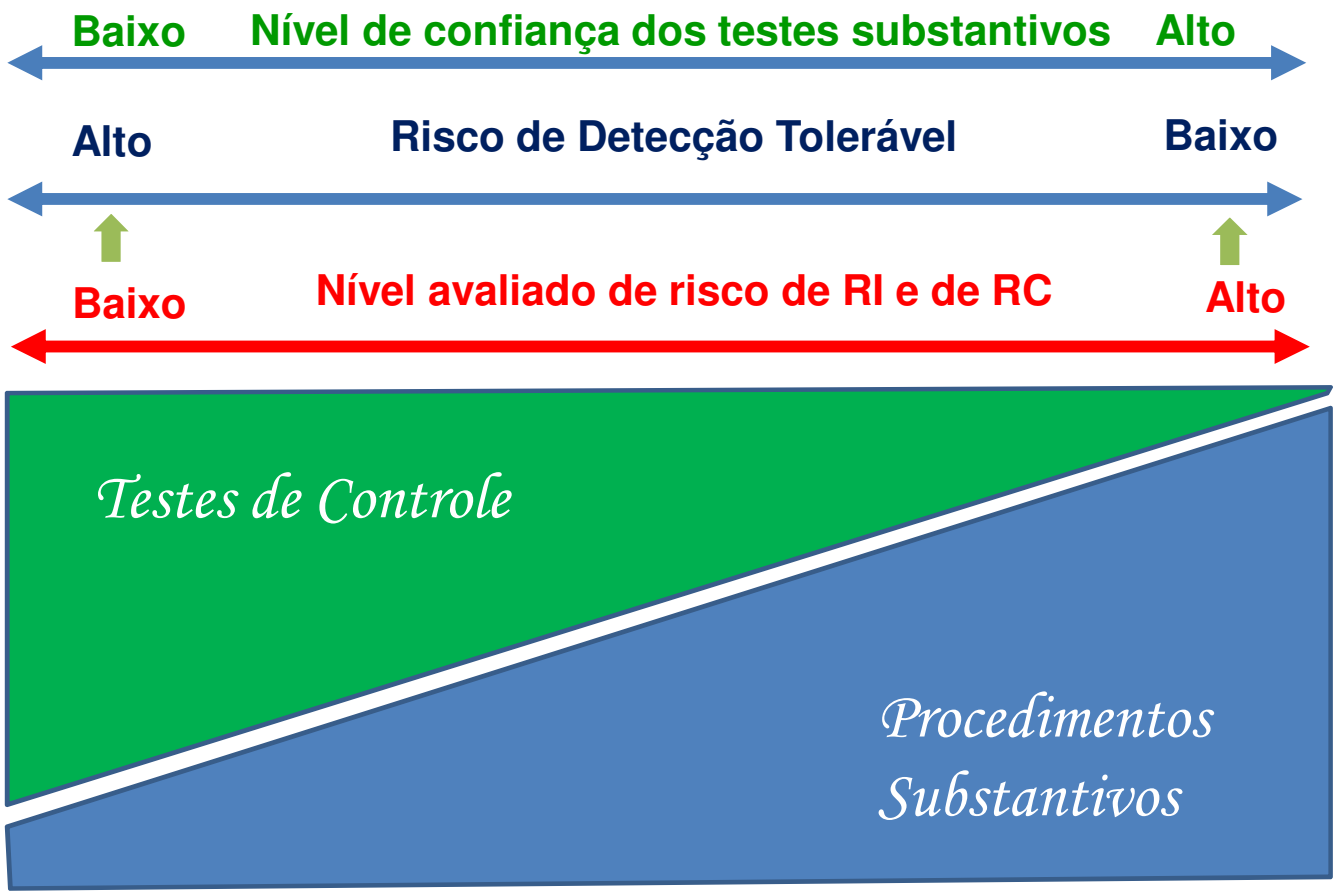
Matriz de Avaliação de Riscos

PROCESSO:

OBJETIVOS-CHAVE DO PROCESSO:

ATIVIDADES DE EXECUÇÃO			RISCO INERENTE				ATIVIDADES DE CONTROLE				RISCO RESIDUAL	
SEQ.	DESCRIÇÃO	RESP.	DESCRIÇÃO	I	P	RI	DESCRIÇÃO	RESP.	AC	RC	RDR	TESTES DE AUDITORIA
			R1 -									
			R2 -									
			R3									

Abordagem de Auditoria



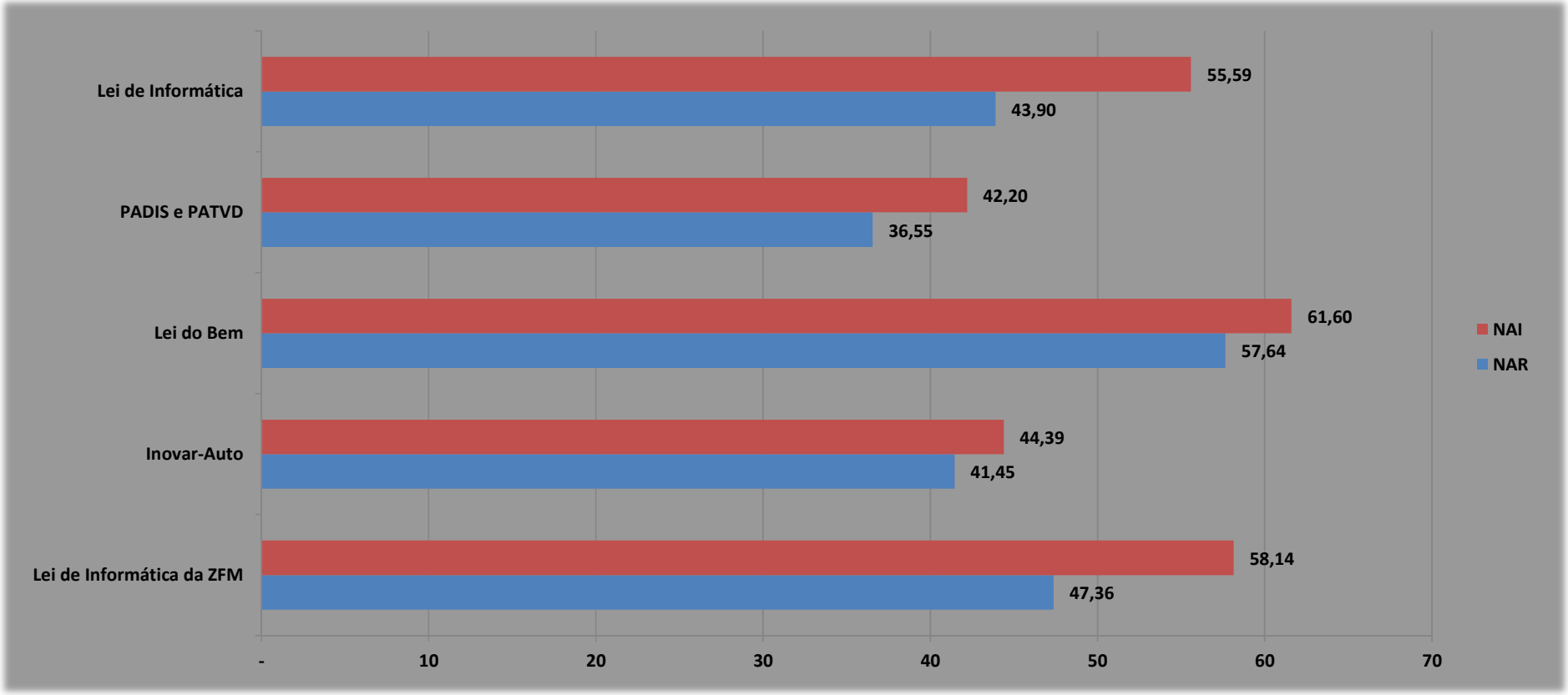
Procedimentos

1. Identificação dos riscos inerentes
2. Análise dos riscos inerentes (RI = I x P)
3. Identificação dos controles que mitigam os riscos inerentes
4. Avaliação do desenho dos controles e dos riscos residuais
5. Elaboração do Programa de Auditoria Baseado em Risco
   - Procedimentos de testes EOC controles e procedimentos substantivos)
6. Fase Execução
7. Fase Relatório

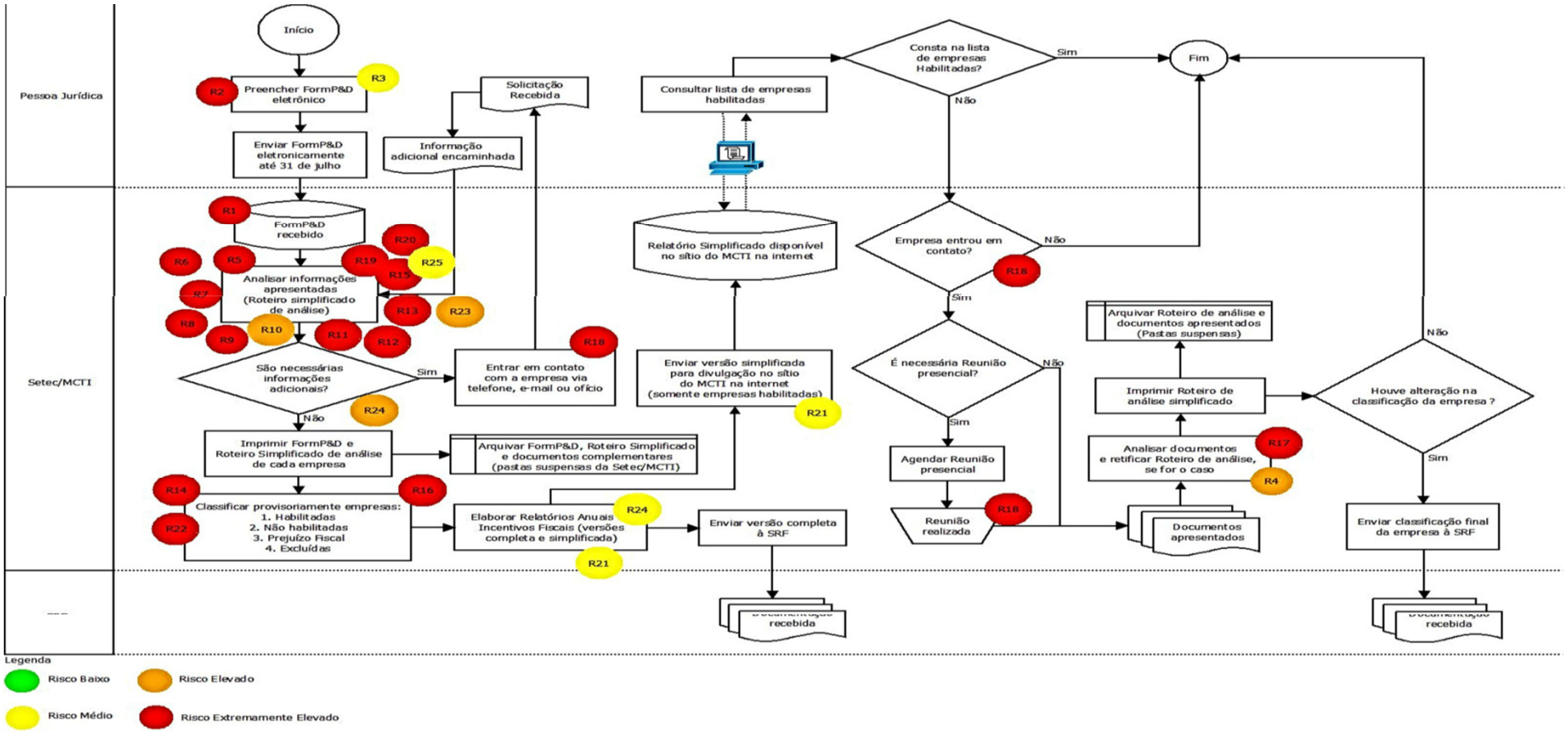
Elaboração do programa de auditoria

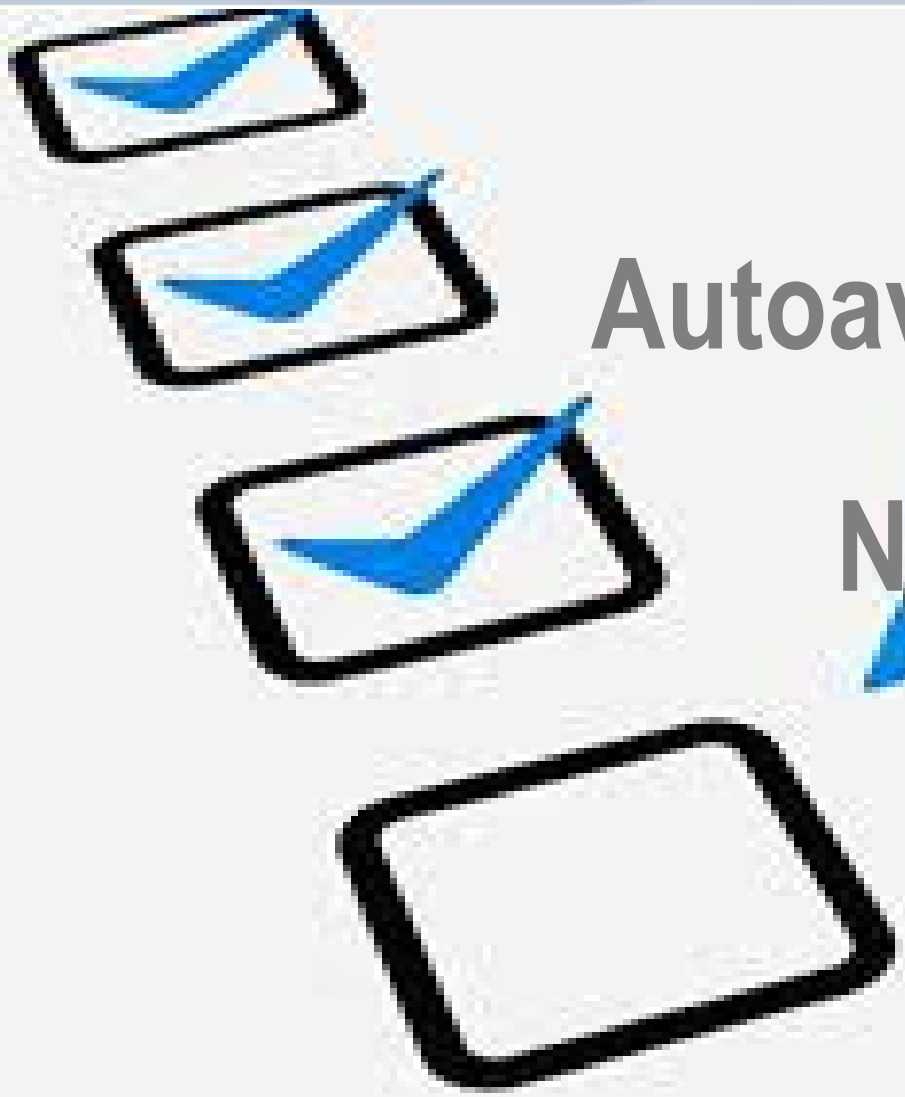
- Norma 2240 –Programa de Trabalho de Auditoria
  - Os auditores internos devem desenvolver e documentar programas de trabalho que atendam os objetivos do trabalho.
  - 2240.A1 – Os programas de trabalho devem incluir os procedimentos para **identificar, analisar, avaliar e documentar** as informações durante o trabalho de auditoria. O programa de trabalho **deve ser aprovado** antes de ser implantado e quaisquer ajustes devem ser prontamente aprovados.

Resultados


Lei de Informática
55,59
43,90
PADIS e PATVD
42,20
36,55
Lei do Bem
61,60
57,64
Inovar-Auto
44,39
41,45
Lei de Informática da ZFM
58,14
47,36
NAI
NAR
-
10
20
30
40
50
60
70

Resultados


Pessoa Jurídica
Setec/MCTI
Início
Preencher FormP&D eletrônico
Enviar FormP&D eletronicamente até 31 de julho
FormP&D recebido
Analisar informações apresentadas (Roteiro simplificado de análise)
São necessárias informações adicionais?
Sim
Não
Solicitação Recebida
Informação adicional encaminhada
Entrar em contato com a empresa via telefone, e-mail ou ofício
Imprimir FormP&D e Roteiro Simplificado de análise de cada empresa
Arquivar FormP&D, Roteiro Simplificado e documentos complementares (pastas suspensas da Setec/MCTI)
Classificar provisoriamente empresas:
1. Habilitadas
2. Não habilitadas
3. Prejuízo Fiscal
4. Excluídas
Elaborar Relatórios Anuais Incentivos Fiscais (versões completa e simplificada)
Enviar versão completa à SRF
Consultar lista de empresas habilitadas
Relatório Simplificado disponível no sítio do MCTI na internet
Enviar versão simplificada para divulgação no sítio do MCTI na internet (somente empresas habilitadas)
Consta na lista de empresas Habilitadas?
Fim
Empresa entrou em contato?
É necessária Reunião presencial?
Agendar Reunião presencial
Reunião realizada
Arquivar Roteiro de análise e documentos apresentados (Pastas suspensas)
Imprimir Roteiro de análise simplificado
Analisar documentos e retificar Roteiro de análise, se for o caso
Documentos apresentados
Houve alteração na classificação da empresa ?
Enviar classificação final da empresa à SRF
R1
R2
R3
R4
R5
R6
R7
R8
R9
R10
R11
R12
R13
R14
R15
R16
R17
R18
R19
R20
R21
R22
R23
R24
R25
Legenda
Risco Baixo
Risco Elevado
Risco Médio
Risco Extremamente Elevado



Autoavaliação de Controles

Nível de atividade

Definição e Propósito

- Segundo a literatura do IIA:

A AAC é um processo através do qual a eficácia do controle interno é examinada e avaliada. O objetivo é prover segurança razoável de que todos os objetivos de negócio serão alcançados (IIA, 1998).