

SMART **RISK** **MODEL FRAMEWORK**

Framework da Metodologia
Análise de Risco Parametrizada
2.0

SMART RISK MODEL FRAMEWORK

Índice

1.Introdução

2. Smart Risk Model

2.1. Quadro Sinótico

2.2. Revisão Metodológica

2.3. Definição do Contexto

2.4. Mapeamento & Identificação de Risco

2.5. Critérios de Aceitação de Riscos

2.6. Análise de Riscos

2.7. Mensuração de Riscos

2.8. Avaliação de Riscos

2.9. Apresentação & Resposta a Riscos

2.10. Avaliação do Ambiente de Controle

2.11. Tratamento de Risco

2.12. Monitoramento & Análise Crítica

2.13. Comunicação & Consulta

3. Conclusão

4. Anexo

Tabela Referencial

1.Introdução

O **SMART RISK MODEL FRAMEWORK** é o framework de implantação do modelo de gestão de riscos da metodologia Análise de Risco Parametrizada. Em outras palavras, é a estrutura e o passo a passo para que você possa implantar um programa e uma estrutura de gestão de riscos na sua empresa.

Ele é um modelo gráfico que facilita ao time de gestão de riscos ou de governança corporativa conseguir implementar um modelo de gestão de riscos alinhado com as melhores práticas do mercado (ISO 31.000, COSO ERM, etc....).

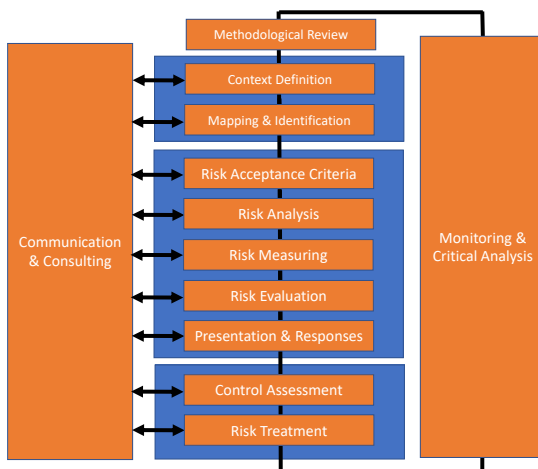
Este e-book visa enfatizar as principais fases da implantação da metodologia **Análise de Risco Parametrizada**. Ele funciona de maneira complementar aos e-books da **Série ERM Fórmula de Implantação de Gestão de Riscos** ou do **Curso Formula de Implantação de Gestão de Riscos**.

Nas páginas a seguir você verá quais são os principais passos para a implantação do modelo com os respectivos descritivos de cada um desses passos. Também serão citadas as principais técnicas utilizadas neste processo. Se você estiver utilizando algum livro da **Série ERM Fórmula de Implantação de Gestão de Riscos** ou realizando o **Curso Formula de Implantação de Gestão de Riscos**, você facilmente conseguirá se situar em que parte do processo de implantação do modelo de gestão de riscos você está vivenciando. Desta forma, você consegue enxergar o que ainda falta na sua estrutura e os principais desafios pela frente. Entendemos que esta abordagem auxilia muito o processo de implantação do modelo e proporciona uma ideia clara dos pontos deficientes neste processo.

2. Smart Risk Model

2.1. Quadro Sinótico

O Quadro Sinótico é a representação gráfica do framework de implantação da metodologia **Análise de Risco Parametrizada**. Por ser uma metodologia baseada, principalmente, nas metodologias COSO ERM e ISO 31.000, possui um framework bem similar ao destas metodologias conforme pode-se observar no desenho abaixo:

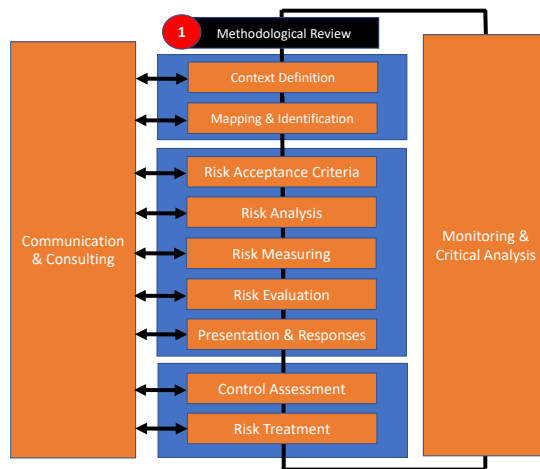


O Quadro Sinótico possibilita que o gestor de riscos seja capaz de verificar todas as etapas do modelo de gestão de riscos, identificar pontos vulneráveis que precisam de mais atenção e entender como cada uma dessas fases interagem entre si.

Este quadro também facilita com que o time de gestão de riscos possa revisar o seu modelo e a própria metodologia, evitando que algum ponto fique esquecido ou passe despercebido durante a revisão.

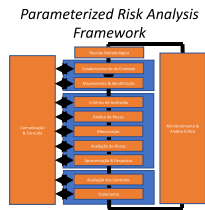
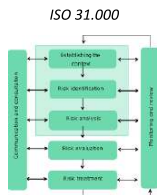
2.2. Revisão Metodológica

A melhor maneira de se conduzir a revisão metodológica é utilizar o Quadro Sinótico pra rever a metodologia. Uma das formas é comparar este framework com os frameworks da ISO 31.000, COSO ERM, etc.... e verificar se ele consegue atender as demandas das normas utilizadas como referência.



Para se ter mais efetividade neste processo de revisão metodológica, pode-se fazer um quadro comparativo que facilite a visualização dos itens que são atendidos por cada uma das metodologias. Isto possibilita que sempre sejam incorporados os melhores conceitos, os melhores princípios e melhores ferramentas de cada metodologia.

Framework: Parameterized Risk Analysis



Comparative Table

Item	COSO ERM	ISO 31.000	ARP
Contexto			
Identificação			
Critérios de Aceitação			
Análise de Riscos			
Mensuração de Riscos			
Avaliação de Riscos			
Avaliação dos Controles			
Monitoramento			
Comunicação & Consulta			

Sugere-se que além das metodologias que servem de base para o framework de gestão de riscos, que outras metodologias, regulações e documentos também sejam utilizados como referência. Dentre elas podemos citar:

Riscos Operacionais

Segurança da Informação: COBIT, ISO 27.000, GDPR, LGPD etc....

Segurança Patrimonial: Protocolos e Documentos da ASIS, NFPA, FM Global, etc....

Segurança do Trabalho: OHSAS 18.000, NFPA, FM Global, etc....

Segurança Ambiental: ISO 14.000, Normas e Regulações Ambientais, etc....

Riscos de Compliance

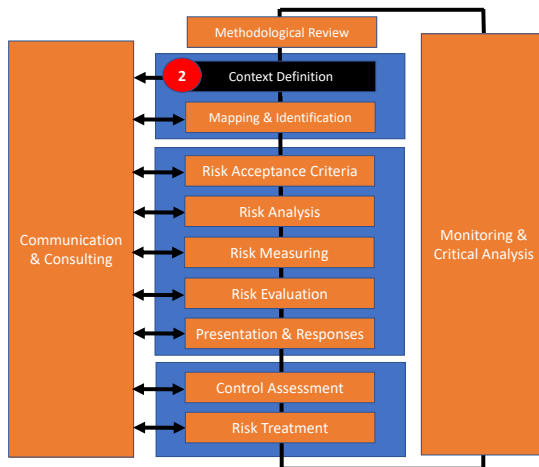
Anticorrupção: UK Bribery Act, FCPA, FACTA, Lei Anticorrupção Brasileira, Memorando de lales, ISO 37.301, etc....

Lavagem de Dinheiro: FACTA, Lei Anticorrupção Brasileira, Normas e Regulações do BACEN, ISO 37.301, etc....

Você encontra mais informações e ferramentas sobre como realizar a Análise do Contexto e Identificação de Riscos Emergentes na plataforma no **Curso / Modulo Fundamentos de Gestão de Riscos** ou no e-book da **Série ERM: Fundamentos de Gestão de Riscos**.

2.3. Definição do Contexto

A Definição do Contexto consiste principalmente em definir e compreender os drivers estratégicos de uma organização.

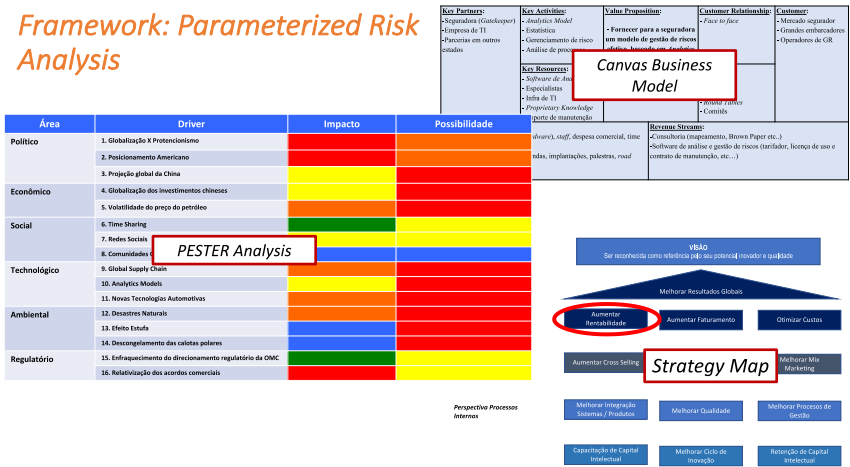


Para se compreender os drivers estratégicos de uma organização é necessário compreender sua missão, sua proposta de valor, o seu modelo de negócio, o mercado em que atua, o tipo de indústria, sua cadeia de valor, seus principais clientes, seus principais fornecedores e o ambiente em que está imersa.

Para entender de forma correta este ambiente do qual a empresa faz parte, é necessário identificar e analisar as principais macrotendências no campo político, econômico, social, tecnológico, ambiental e regulatório.

Além disso, precisa-se avaliar qual a possibilidade destas tendências virem a se concretizar e quais são os riscos emergentes destas mudanças bruscas nos campos político, econômico, social, tecnológico, ambiental e regulatório. Deve-se também analisar quanto estes riscos emergentes de fato podem afetar de maneira contundente a organização.

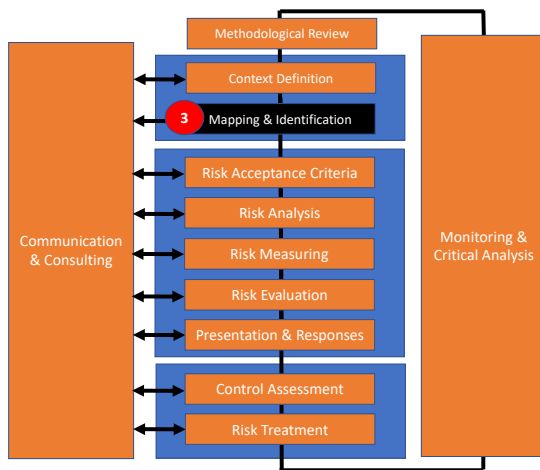
Framework: Parameterized Risk Analysis



Você encontra mais informações e ferramentas sobre como realizar a Análise do Contexto e Identificação de Riscos Emergentes na plataforma no **Curso / Módulo Mapeamento e Identificação de Riscos** ou no e-book da **Série ERM: Mapeamento e Identificação de Riscos**.

2.4. Mapeamento & Identificação de Risco

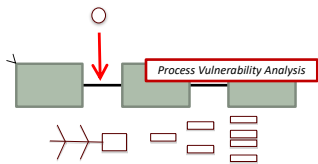
Esta fase consiste basicamente em realizar o mapeamento, identificação e descrição dos riscos críticos. Ela é considerada crítica porque todas as demais fases baseiam-se nos resultados obtidos nesta fase para darem prosseguimento nas análises, avaliações e conclusões subsequentes.



Nesta fase aplicamos ferramentas, tais como: entrevista de riscos, workshop de riscos, definição do Worst-Case Scenario entre outros. Além disso, é levada em consideração os resultados da análise de cenários, que normalmente é conduzida na fase anterior.

Após mapear e identificar os riscos, o time de gestão de riscos deve, de maneira bastante criteriosa, listar os riscos críticos da organização e fazer a definição do seu Worst-Case Scenario utilizando a técnica adequada para tal.

Framework: Parameterized Risk Analysis



Key Partners: Seguradora (underwriter) Empresas de TI Pacientes em outros estados	Key Activities: Analytics Model Estatística Gerenciamento de risco Análise de percepções	Value Proposition: - Fornecer para a seguradora um modelo de gestão de riscos eficiente, baseado em dados.	Customer Relationship: - Face-to-face	Channels: - Mercado segurador - Grandes embarcadores - Operadores de CR
Canvas Business Model (Risk Analysis)				
Key Resources: - Modelo Definitivo (Estatísticas / Analytics) - Dados de Risco Definitivo (gestão operacional definitiva, indicadores mal definidos, gaps de competências essenciais etc.)				
Key Activities: - Custo Fixo: TI (incluindo especialistas) - Custo variável: consultores etc. Economia de escala				

Tema / Driver	Ameaça	Risco Corporativo
1. Globalização X Protecionismo	- Barreiras alfandegárias / impostos restritivos	Perda de Market Share
2. Posicionamento Americano	- Não cumprimento de acordos comerciais - Barreiras alfandegárias / impostos restritivos	Perda de Market Share
3. Projeção global da China	- Novos entrantes chineses nas áreas de infraestrutura e O&G	Sem impacto para o negócio
4. Globalização dos investimentos chineses	- Novos entrantes chineses nas áreas de infraestrutura e O&G	Sem impacto para o negócio
5. Volatilidade do preço do petróleo	PESTER Risk Analysis	Crise de Margem de lucro
7. Redes Sociais	- Impacto das redes sociais nos hábitos de consumo	Sem impacto para o negócio
9. Analytics Models	- Geração de modelos disruptivos de negócio	Sem impacto para o negócio
12. Desastres Naturais	- Interrupção da cadeia de suprimento	Desabastecimento
12. Global Supply Chain	- Interrupção da cadeia devido desastres naturais	Desabastecimento
16. Renovação dos acordos comerciais	- Não cumprimento de acordos comerciais - Barreiras alfandegárias / sobretaxas / impostos restritivos	Perda de Market Share



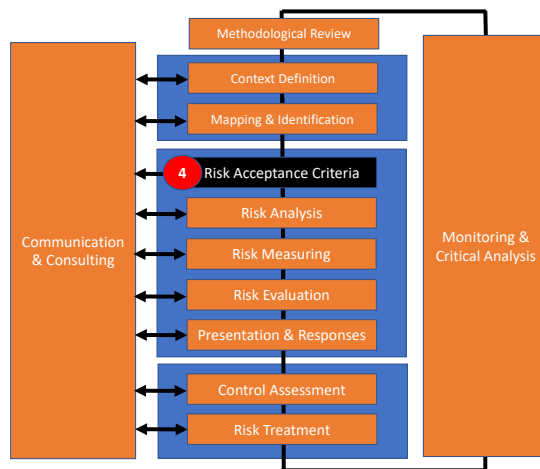
Você encontra mais informações e ferramentas sobre como realizar o Mapeamento e Identificação de Riscos na plataforma no **Curso / Módulo Mapeamento e Identificação de Riscos** ou no e-book da **Série ERM: Mapeamento e Identificação de Riscos**.

2.5. Critérios de Aceitação de Riscos

Nesta fase, o profissional de gestão de riscos, juntamente com o conselho e representantes da alta gestão, devem realizar a definição dos critérios de aceitação de riscos. Principalmente a Definição de **Apetite a Risco**.

A definição dos critérios de aceitação de riscos define os parâmetros de riscos a serem aceitos por uma organização. Somente por meio da definição dos critérios de aceitação de riscos que os gestores da organização conseguem ter uma ideia de quais riscos eles devem aceitar ou recusar quando forem definir uma estratégia.

Os gestores de riscos baseiam-se na definição dos critérios de aceitação de riscos para definirem como será o modelo de gestão de riscos a ser adotado pela organização. Quanto mais rígidos forem os critérios de aceitação de riscos, mais rígido será o modelo de gestão de riscos a ser adotado e o ambiente de controle a ser implementado (controles mais rígidos).



Esta fase aborda temas e ferramentas para a definição de Appetite a Risco, definição do Limite de Tolerância a Risco, capacidade de retenção de risco, Máxima Perda Admissível, entre outros.

Framework: Parameterized Risk Analysis

Risk Profile			
Category of Risk		Appetite (Level)	
Operational			
Strategic		Risk Profile	
		Low	
		Moderated	

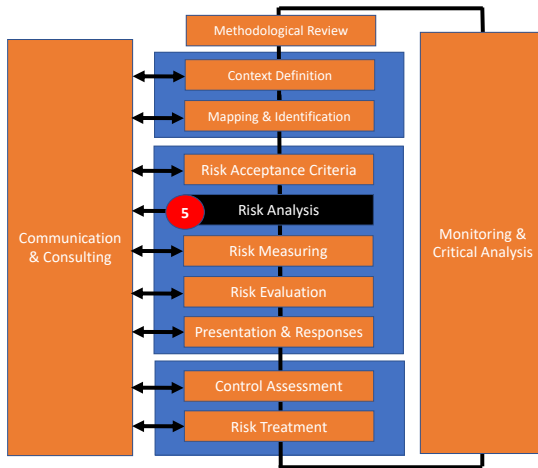
Risk Category	Risk Sub-category	Appetite (Level)	Risk Appetite Statement
Operacional	Nuclear Accident		Our operational risk appetite is considered very high . We recognize the risks involved in operating nuclear power plants. Their consequences can be devastating.
			We do not accept any reckless behavior related to safety or security procedure.
			We have been operating nuclear plants for more than 30 years without any major accident or incident. We are not expecting any major ones in the next 20 years from now on.
			To control this level of risk, we have strict procedures, regular training, external overseeing led by the USSR Nuclear Agency and redundancy systems.

Risk Appetite Description

Você encontra mais informações e ferramentas sobre como realizar a definição dos Critérios de Aceitação de Riscos na plataforma no **Curso / Modulo Critérios de Aceitação de Riscos: *Apetite & Tolerância*** ou no e-book da **Série ERM: Critérios de Aceitação de Riscos**.

2.6. Análise de Riscos

Esta é a fase na qual o profissional de gestão de riscos começa a aprofundar a análise dos riscos críticos. Ele detalha as análises primarias que já foram realizadas dos seus riscos críticos. Normalmente, busca-se ter uma noção mais abrangente do impacto dos riscos e de suas causas. Também é feita uma análise detalhando mais as perdas diretas e quais são as perdas indiretas de cada risco crítico.



Diversas ferramentas utilizadas nas fases anteriores são revisadas e suas informações são detalhadas ou complementadas com objetivo de se ter uma visão mais precisa da abrangência dos riscos.

Framework: Parameterized Risk Analysis

Losses				
Direct		Indirect		Total Loss
Item	R\$	Item	R\$	R\$
Buildings	40 millions	Fines due not to accomplish SLA	35 millions	75 millions
Machinery	70 million	Loss Matrix		20 millions
Inventory	50 million			50 millions
Total	160 millions		85 millions	245 millions

Scenario Matrix		
Risk 01:		
Risk Description (Worst-Case Scenario)		
Impact on Critical Variables		
Environmental	Media & Image	Population / Community
Final	Scenario Matrix & Impacts	
Staff	Assets	Business

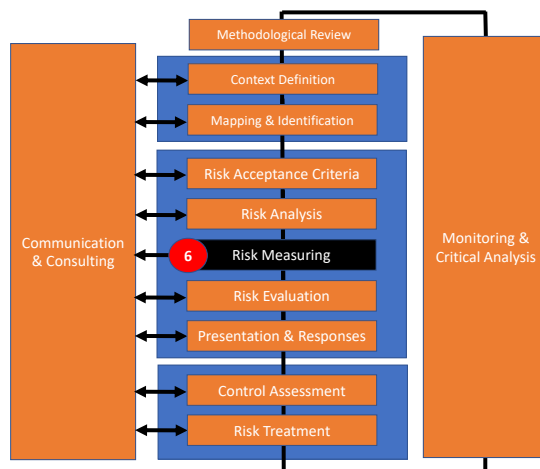
Causes	Consequences

Bow-Tie Analysis	
------------------	--

Você encontra mais informações e ferramentas sobre como realizar o Análise de Riscos na plataforma no **Curso / Modulo Avaliação de Riscos: Análise & Mensuração** ou no e-book da **Série ERM: Avaliação de Riscos: Análise & Mensuração**.

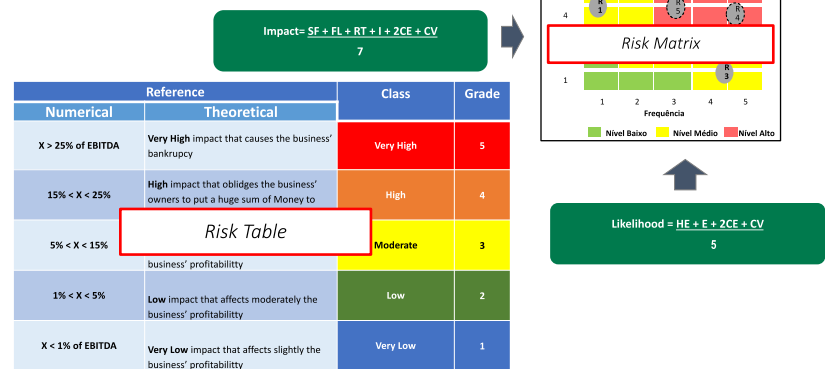
2.7. Mensuração de Riscos

Na fase de Mensuração de Riscos é a fase na qual é feita a mensuração dos riscos por meio de modelos qualitativos utilizando-se tabelas de riscos para a confecção de uma Matriz de Riscos da organização.



Ainda nesta fase, o time de gestão de riscos define quais as variáveis críticas que são impactadas pelos riscos (para quantificar seu impacto) e quais contribuem para a sua ocorrência (para definir a sua possibilidade de ocorrer). Também aborda questões mais complexas como é o caso da definição das variáveis complementares.

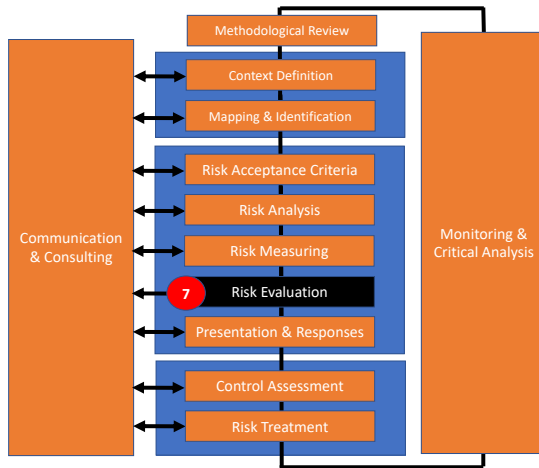
Framework: Parameterized Risk Analysis



Você encontra mais informações e ferramentas sobre como realizar a Mensuração de Riscos na plataforma no **Curso / Modulo Avaliação de Riscos: Análise & Mensuração** ou no e-book da **Série ERM: Avaliação de Riscos: Análise & Mensuração**.

2.8. Avaliação de Riscos

A principal característica desta fase consiste em comparar os resultados obtidos nas diversas análises e na mensuração dos riscos com os critérios de aceitação de riscos definidos na organização.



Este processo fornece informações e ferramentas para o gestor de riscos fazer uma análise crítica bem estruturada e embasada de cada risco crítico tendo como parâmetros o nível de apetite e tolerância já definidos. Desta forma, o gestor de riscos terá segurança suficiente para apresentar ao conselho e para a alta gestão da empresa as alternativas existentes para lidar com cada um dos riscos tendo como base os critérios de aceitação de riscos da organização.

Framework: Parameterized Risk Analysis

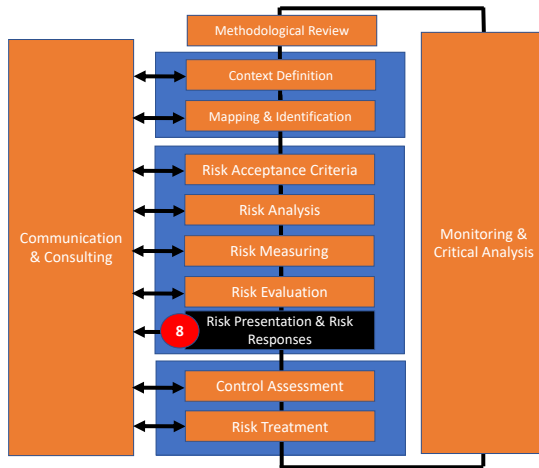


Você encontra mais informações e ferramentas sobre como realizar a Avaliação de Riscos na plataforma no **Curso / Modulo Avaliação de Riscos: Análise & Mensuração** e no **Curso / Modulo Apresentação de Riscos** ou nos e-books da **Série ERM: Avaliação de Riscos: Análise & Mensuração** e **Série ERM: Apresentação de Riscos**.

2.9. Apresentação & Resposta a Riscos

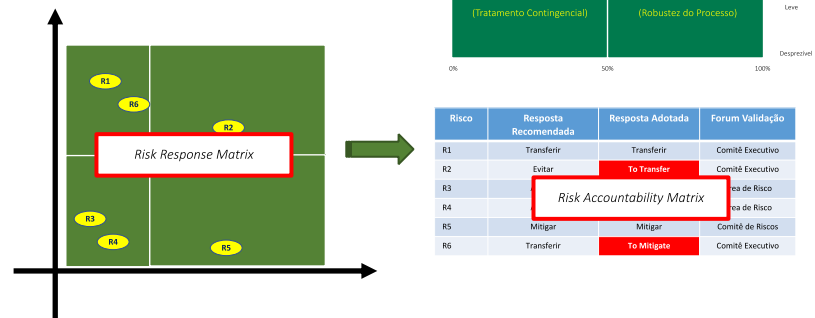
Nesta fase, o gestor de riscos, após ter feito uma avaliação técnica detalhada dos riscos críticos de sua organização e tendo comparado os efeitos de cada um destes riscos com os critérios de aceitação da organização, ele estrutura a melhor maneira de apresentá-los ao conselho e a alta gestão da organização.

Durante a apresentação dos riscos, o gestor de riscos deve indicar e obter uma validação inicial das formas de tratamento destes riscos apresentados (ainda que de maneira macro). Estas formas de tratamento levarão em consideração as 4 respostas clássicas a riscos: Evitar, Aceitar, Mitigar e Transferir.



O gestor de riscos deve fazer uma análise multifacetada de cada riscos, ou seja, analisando os riscos por diferentes perspectivas, utilizando diversas ferramentas e da forma mais holística possível. Entre os principais temas e ferramentas disponíveis utilizados para a apresentação de riscos temos: Matriz de Riscos, Matriz de Vulnerabilidades, Heat Map de Vulnerabilidades, Matriz de Resiliência Financeira, etc...

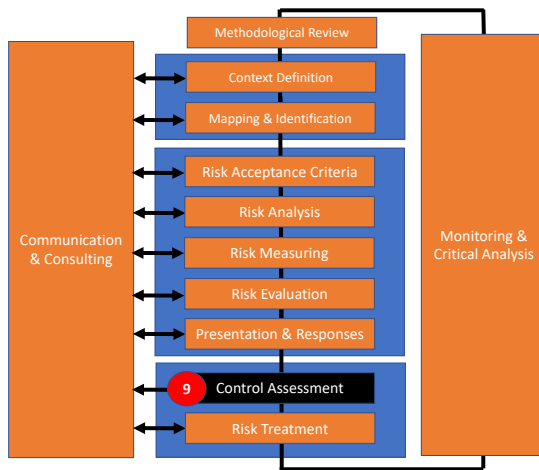
Framework: Parameterized Risk Analysis



Você encontra mais informações e ferramentas sobre como realizar a Apresentação de Riscos e a Definição de Respostas a Riscos na plataforma no **Curso / Modulo Avaliação de Riscos: Análise & Mensuração** e no **Curso / Modulo Apresentação de Riscos** ou nos e-books da **Série ERM: Avaliação de Riscos: Análise & Mensuração e Série ERM: Apresentação de Riscos**.

2.10. Avaliação do Ambiente de Controle

Nesta fase, o profissional de gestão de riscos realiza a avaliação do ambiente de controle de sua organização. Ele verifica se para cada risco crítico existe um ambiente de controle adequado. Ele realiza auditorias nos ambientes de controles a fim de identificar vulnerabilidades críticas a serem corrigidas.

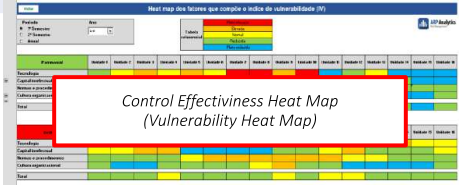


Através da correta avaliação do ambiente de controle é que o gestor de riscos irá conseguir definir as principais ações para mitigar os riscos de forma efetiva. Dentre os principais métodos existentes para a avaliação da efetividade do ambiente de controle temos: o Método Sumário, o Método Estruturado e o Método Paramétrico de avaliação do Ambiente de Controle.

Framework: Parameterized Risk Analysis

Risco Crítico	Grupo	Controle / Mecanismo de Proteção	Norma / Especialista	Grupo de Parâmetros
Invasão Hacker	Segurança da Informação	Sistema de Segurança da Informação	ISO 27.000 / COBIT / GDPR	Segurança da Informação
Corrupção de Funcionário público	Compliance	Programa de Compliance	UKBA / FCPA / LACBRA / Memorando lists	Compliance Anti-corrupção
Perda de Market Share				Inteligência de Marketing
Invasão do site da empresa				Segurança Patrimonial
Incêndio	Patrimonial	Sistema Contra Incêndio	NFPA / FM Global	Incêndio
Fuga Voluntária de Informação	Capital Intelectual	Sistema de Avaliação de Aderência	Ribeiro & Santos	Avaliação de Aderência

Correlation Matrix: Risks & Control Environment



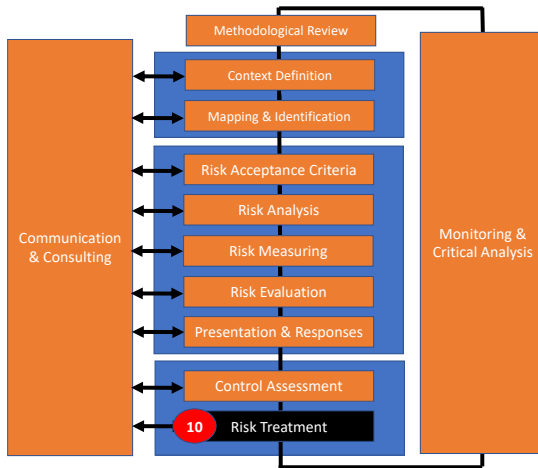
Item		Descrição	A. Exatidão (20 itens)										Totais
43	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações
44	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações
45													
46													
47	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações
48	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações
49	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações
50	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações
51	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações
52	3.4	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações	Exatidão da informação de segurança de informações

Parametric Check List

Você encontra mais informações e ferramentas sobre como realizar a Avaliação do Ambiente de Controle na plataforma no **Curso / Modulo Avaliação do Ambiente de Controle** ou no e-book da **Série ERM: Avaliação do Ambiente de Controle**.

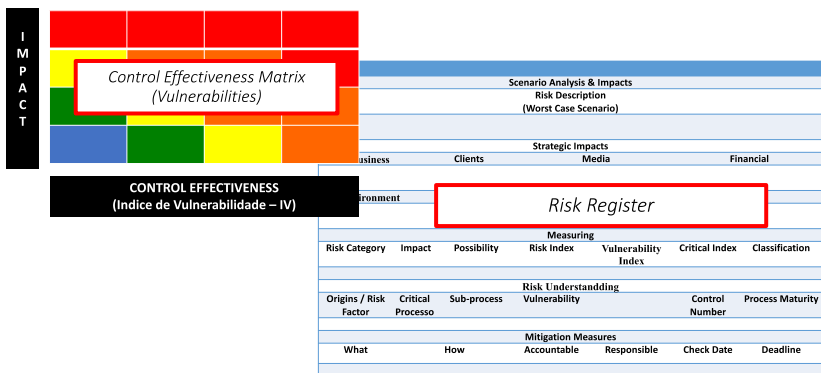
2.11. Tratamento de Risco

Nesta fase, é que são aplicadas as 4 respostas clássicas a riscos: Evitar, Aceitar, Mitigar e Transferir. Uma vez tendo sido definido o tratamento, o time de gestão de riscos vai definir como será feita a operacionalização da resposta ao risco.



Durante este processo o profissional de gestão de riscos deve considerar como estabelecer medidas para mitigar e transferir os riscos de forma adequada. Ele deve implantar ferramentas para implementar um robusto processo de mitigação de riscos em sua organização. Algumas ferramentas importantes, tais como: Diagrama de Causa-Efeito, 5W2H e Ficha de Risco devem ser utilizadas para se ter um processo de mitigação de riscos efetivo.

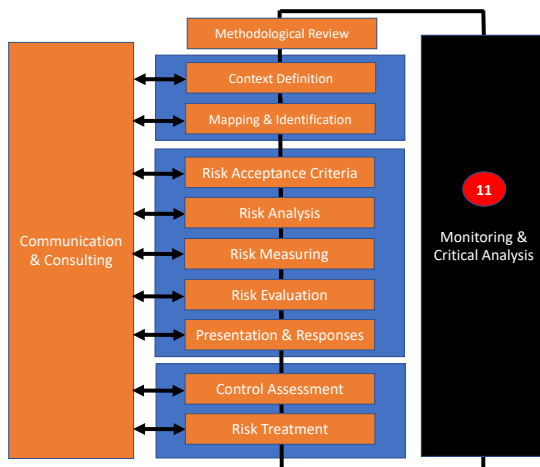
Framework: Parameterized Risk Analysis



Você encontra mais informações e ferramentas sobre como realizar o Tratamento dos Riscos na plataforma no **Curso / Modulo Apresentação de Riscos** e no **Curso / Modulo Mitigação de Riscos** ou nos e-books da **Série ERM: Apresentação de Riscos** e da **Série ERM: Mitigação de Riscos**.

2.12. Monitoramento & Análise Crítica

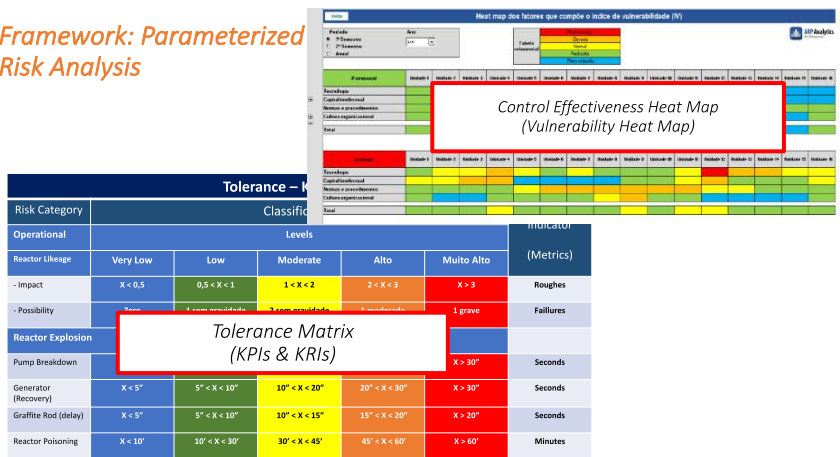
O monitoramento e a análise crítica devem ocorrer durante todo o processo de gestão de riscos. Para se fazer uma correta análise crítica em gestão de riscos, o time de gestão de riscos precisa ter uma correta noção dos princípios, dos conceitos e dos axiomas de gestão de riscos. Também devem ser empregadas ferramentas para que seja feito o monitoramento dos riscos. Elas darão a transparência necessária para o gestor de riscos poder acompanhar os riscos e fazer a sua análise crítica dos mesmos.



Durante este processo também se apresenta uma abordagem de como avaliar o nível de maturidade de gestão de riscos em uma organização. Também discorre sobre a diferença entre gestão e governança de riscos, bem como sobre o papel e a importância do Comitê de

Gestão de Riscos. Além disso, é implementado o Comitê de Gestão de Riscos tendo entre suas funções o acompanhamento dos riscos críticos e conduzir análises críticas sobre o modelo de gestão de riscos e as estratégias adotadas para lidar com o tema.

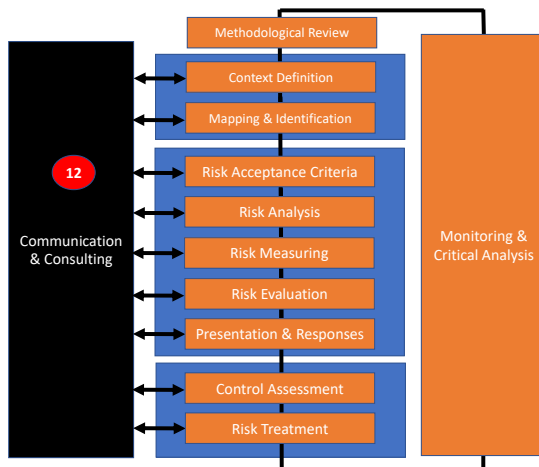
Framework: Parameterized Risk Analysis



Você encontra mais informações e ferramentas sobre como realizar o Monitoramento e a Análise Crítica dos Riscos na plataforma no **Curso / Modulo Fundamentos de Gestão de Riscos**, no **Curso / Modulo Mitigação de Riscos** e no **Curso / Modulo Maturidade & Governança** ou nos e-books da **Série ERM: Fundamentos de Gestão de Riscos**, **ERM: Mitigação de Riscos** e **ERM: Maturidade & Governança**.

2.13. Comunicação & Consulta

Estas ações ocorrem durante todo o processo de gestão de riscos. Através de políticas, diretrizes, normas, dos planos críticos e da atuação do Comitê de Gestão de Riscos que é exercido o processo de comunicação e consulta da área de gestão de riscos com a organização.



As Políticas de Gestão de Riscos, os relatórios de acompanhamento regulares, e os Planos Críticos (Plano de Gestão de Riscos, Plano de Contingência, Plano de Gestão de Crises e Plano de Continuidade do Negócio) são ferramentas que apresentam uma forma bastante objetiva e efetiva para se realizar a comunicação. Esta comunicação deve ser acompanhada de feedbacks regulares e de ações de melhoria de processo.

A ação do Comitê de Gestão de Riscos fazendo um acompanhamento e cobrança constante é um fator primordial neste processo. Neste comitê é possível discutir em profundidade e com abrangência diversos temas ligados a gestão de riscos da organização.

Os feedbacks obtidos nos processos de consultas realizados junto as demais áreas da organização ou junto ao Comitê de Gestão de Riscos possibilita que o gestor de riscos possa fazer os ajustes adequados na Política de Gestão de Riscos e no seu Modelo de Gestão de Riscos a fim de obter mais aderência as necessidades da empresa e maior efetividade.

Framework: Parameterized Risk Analysis

Risk Management Program		
Item	Status	Main Recommendations
Context		To carry out PESTER Analysis
Risk Identification		To improve thhe risk interview process
Risk Acceptance Criteria: Appetite / Tolerance		To redefine the risk acceptance criteria
Risk assessment		To review theoretical references (Risk Boards)
Risk Holistic Anal	Systematic Review	
Risk Responses		
Control Effectiveness		
Risk Mitigation		To review risk registers
Risk Transference		To review estimated losses and insurance coverage
Risk Governance		To review KPIs / KRIs
Risk Committée		To review the Risk Management Policy
Sistematic Review		To build the Risk Maturity check list

Você encontra mais informações e ferramentas sobre como realizar a Comunicação & Consulta de Riscos na plataforma no **Curso / Modulo Apresentação de Riscos**, **Curso / Modulo Planos Críticos** e no **Curso / Modulo Maturidade & Governança** ou nos e-books da **Série ERM: Apresentação de Riscos**, da **Série Planos Críticos** e da **Série ERM: Maturidade & Governança**.

3. Conclusão

O **SMART RISK MODEL FRAMEWORK** nada mais é que um framework de gestão de riscos da metodologia **Análise de Risco Parametrizada**. Ele permite ao gestor identificar todas as fases do seu processo de gestão de riscos bem como identificar inconsistências ou vulnerabilidades nesses processos.

Recomendamos que as análises feitas com a utilização do **SMART RISK MODEL FRAMEWORK** sejam acompanhadas pela revisão da metodologia **Análise de Risco Parametrizada**. Isto pode ser feito por meio da leitura da metodologia ou pelo acesso a plataforma onde se encontram e-books, videoaulas e templates para implantação da metodologia. Para tal, disponibilizamos no anexo desta obra uma tabela referencial com os links online que direcionam ao material de apoio.

Em especial, os templates disponíveis na plataforma favorecem sobremaneira o processo de implantação deste modelo de gestão de riscos nas organizações. Pouparam tempo do time de gestão de riscos e previnem que algum item seja esquecido durante o processo de implantação do modelo de gestão de riscos ou durante o processo de revisão do modelo de gestão de riscos já existente.

4. Anexo

Tabela Referencial

Endereços Online		
Tema	Cursos Relacionados	E-books Relacionados
Revisão Metodológica	Fundamentos de Gestão de Riscos https://www.arpdigitalconsulting.com	Série ERM: Fundamentos de Gestão de Riscos https://www.arpdigitalconsulting.com/cursos
Definição do Contexto	Mapeamento e Identificação de Riscos https://www.arpdigitalconsulting.com	Série ERM: Mapeamento e Identificação de Riscos https://www.arpdigitalconsulting.com/cursos
Mapeamento & Identificação de Riscos	Mapeamento e Identificação de Riscos https://www.arpdigitalconsulting.com	Série ERM: Mapeamento e Identificação de Riscos https://www.arpdigitalconsulting.com/cursos
Critérios de Aceitação de Riscos	Critérios de Aceitação de Riscos https://www.arpdigitalconsulting.com	Série ERM: Critérios de Aceitação de Riscos https://www.arpdigitalconsulting.com/cursos
Análise de Riscos	Avaliação de Riscos: Análise & Mensuração https://www.arpdigitalconsulting.com	Série ERM: Avaliação de Riscos: Análise & Mensuração https://www.arpdigitalconsulting.com/cursos
Mensuração de Riscos	Avaliação de Riscos: Análise & Mensuração https://www.arpdigitalconsulting.com	Série ERM: Avaliação de Riscos: Análise & Mensuração https://www.arpdigitalconsulting.com/cursos
Avaliação de Riscos	Avaliação de Riscos: Análise & Mensuração Apresentação de Riscos https://www.arpdigitalconsulting.com	Série ERM: Avaliação de Riscos: Análise & Mensuração Série ERM: Apresentação de Riscos https://www.arpdigitalconsulting.com/cursos
Apresentação & Resposta a Riscos	Apresentação de Riscos https://www.arpdigitalconsulting.com	Série ERM: Apresentação de Riscos https://www.arpdigitalconsulting.com/cursos
Avaliação do Ambiente de Controle	Avaliação do Ambiente de Controle https://www.arpdigitalconsulting.com	Série ERM: Avaliação do Ambiente de Controle https://www.arpdigitalconsulting.com/cursos
Tratamento de Riscos	Apresentação de Riscos Mitigação de Riscos https://www.arpdigitalconsulting.com	Série ERM: Apresentação de Riscos Série ERM: Mitigação de Riscos https://www.arpdigitalconsulting.com/cursos
Monitoramento & Análise Crítica	Fundamentos de Gestão de Riscos Mitigação de Riscos Maturidade & Governança https://www.arpdigitalconsulting.com	Série ERM: Fundamentos de Gestão de Risco Série ERM: Mitigação de Riscos Série ERM: Maturidade & Governança https://www.arpdigitalconsulting.com/cursos
Comunicação & Consulta	Apresentação de Riscos Planos Críticos Maturidade & Governança https://www.arpdigitalconsulting.com	Série ERM: Apresentação de Riscos Série ERM: Planos Críticos Série ERM: Maturidade & Governança https://www.arpdigitalconsulting.com/cursos