MERC GROUP

THINK GROWTH. THINK MERC.

GOVERNANÇA DE RISCOS

Gerenciamento de riscos *corporativos* o papel do conselho

Gerenciamento de riscos corporativos define o apetite, as três linhas e a trilha de decisão. Veja o que o conselho responde e o que a auditoria examina.

NORMA BASE	PÚBLICO	EDIÇÃO	DATA
Gerenciamento de riscos e três linhas	Conselhos, comitês de auditoria e gestão de riscos	Guia técnico	Novembro de 2026

O gerenciamento de riscos corporativos é a estrutura pela qual uma organização identifica, avalia, trata e monitora os riscos que podem afetar seus objetivos, e a responsabilidade por essa estrutura é do conselho de administração, não do departamento que a opera. Diferente do controle interno, que cuida da confiabilidade do reporte e da conformidade em processos específicos, o gerenciamento de riscos olha a organização inteira: define o apetite ao risco, estabelece como as decisões incorporam esse apetite e cria as linhas de responsabilidade que separam quem assume o risco de quem o controla e de quem o avalia de forma independente. Para uma instituição financeira, um fundo ou uma fintech regulada, essa estrutura deixou de ser discurso e virou objeto de exame.

A referência de mercado para desenhar essa estrutura é o modelo das três linhas, articulado com uma visão de risco corporativo que vai além do controle contábil. A primeira linha é a área de negócio, que assume e gerencia o risco no dia a dia. A segunda é a função de riscos e de conformidade, que estabelece políticas e monitora. A terceira é a auditoria interna, que avalia de forma independente a eficácia das duas primeiras. A auditoria independente externa não substitui nenhuma delas, mas examina se a estrutura descrita existe de fato e produz evidência. Para discutir a maturidade do seu modelo de riscos, o caminho é o contato.

GOVERNANÇA DE RISCOS

Resumo

O gerenciamento de riscos corporativos é responsabilidade do conselho e trata da organização inteira, enquanto o controle interno cuida da confiabilidade do reporte e da conformidade em processos específicos. Confundir os dois leva a uma estrutura que parece completa e não cobre o risco certo.

O apetite ao risco é o elo que falta na maioria das estruturas imaturas: sem um apetite definido e comunicado, as decisões de negócio não têm parâmetro, e o monitoramento vira registro de eventos sem consequência.

O modelo das três linhas só funciona quando as responsabilidades estão de fato separadas, com a segunda linha independente da primeira e a auditoria interna com acesso direto ao conselho ou ao comitê de auditoria.

A densidade regulatória de 2026, com novas réguas de conduta, de prevenção à fraude, de perda esperada e de capital, eleva a responsabilidade do conselho sobre a estrutura de riscos e torna a trilha de decisão um ponto que a auditoria examina.

P	A
Escopo	A organização e seus objetivos como um todo
Responsável máximo	Conselho de administração
Pergunta central	Quais riscos aceitamos correr e dentro de que limite

P	A
Instrumento típico	Apetite ao risco, políticas e as três linhas

APETITE AO RISCO

O apetite ao risco é o elo que costuma faltar

Em estruturas de risco imaturas, o documento que mais falta não é a matriz de controles, e sim a declaração de apetite ao risco. Apetite ao risco é a definição, aprovada pelo conselho, de quanto e que tipo de risco a organização está disposta a assumir na busca de seus objetivos, traduzida em limites que descem até a operação. Sem ela, o gerenciamento de riscos vira um inventário: a organização lista riscos, atribui probabilidades e impactos, monta mapas de calor, mas nada disso tem consequência, porque não há parâmetro que diga quando um risco ultrapassou o limite tolerado e exige ação.

Quando o apetite existe e é comunicado, a lógica se inverte. As decisões de negócio passam a ser tomadas contra um limite conhecido, o monitoramento ganha gatilhos objetivos e a reportação ao conselho deixa de ser uma coleção de eventos para virar uma leitura de posição frente ao apetite. Esse é o ponto que distingue uma estrutura que gerencia risco de uma que apenas o documenta, e é também o primeiro lugar onde um exame independente percebe se a governança de riscos é real ou decorativa.

TRÊS LINHAS

As três linhas só funcionam separadas

O modelo das três linhas é simples de desenhar e difícil de sustentar, porque sua eficácia depende de separação real de responsabilidades. A primeira linha, o negócio, assume o risco e responde por geri-lo dentro dos limites. A segunda linha, riscos e conformidade, estabelece as políticas, calibra os limites e monitora, e precisa ter independência suficiente da primeira para dizer não. A terceira linha, a auditoria interna, avalia se as duas primeiras funcionam, e precisa de acesso direto ao conselho ou ao comitê de auditoria para que sua avaliação não seja filtrada por quem ela avalia.

A falha típica não é a ausência das linhas, mas a sua sobreposição. Quando a mesma área assume o risco e monitora o próprio limite, a segunda linha não existe na prática. Quando a auditoria interna se reporta a quem deveria auditar, a terceira linha perde independência. Em organizações menores, em que não há estrutura para três áreas separadas, a saída não é fingir que elas existem, e sim desenhar salvaguardas que supram a separação, com revisões independentes e alçadas claras, e documentar essa escolha. A estrutura precisa ser proporcional ao porte, mas a lógica de separação precisa estar presente de alguma forma.

P	A
Primeira linha	Negócio, que assume e gerencia o risco no dia a dia
Segunda linha	Riscos e conformidade, que define políticas e monitora
Terceira linha	Auditoria interna, que avalia a eficácia das duas primeiras
Conselho e comitê	Aprova o apetite e supervisiona a estrutura

2026

Por que 2026 elevou a responsabilidade do conselho

O ano de 2026 concentrou obrigações que, somadas, cobram mais da estrutura de riscos do que qualquer uma delas isolada. As novas réguas de conduta no crédito e no relacionamento com o cliente, as exigências reforçadas de prevenção à fraude nos arranjos de pagamento, a plena incidência do modelo de perda esperada sobre as provisões e a nova metodologia de apuração de capital, com transição ao longo dos próximos exercícios, não são temas de departamentos isolados. Todos pressionam o mesmo ponto: a capacidade do conselho de enxergar a posição de risco da organização e agir dentro de um apetite definido.

O efeito prático é que a estrutura de riscos deixa de ser avaliada apenas por sua existência formal e passa a ser avaliada por sua trilha de decisão. Não basta ter a política e o mapa de riscos; é preciso demonstrar que os alertas chegaram ao conselho, que o conselho deliberou e que a decisão produziu ação. Essa trilha, antes tratada como registro interno, é hoje o que sustenta a afirmação de que a organização gerencia seus riscos, e é por ela que um exame independente começa quando precisa concluir sobre a governança de riscos de uma entidade regulada.

CASO

Um caso anonimizado

Uma instituição de porte médio tinha um arcabouço de riscos completo no papel: política aprovada, mapa de riscos atualizado, comitê instalado. No exame da estrutura, porém, duas coisas apareceram. A declaração de apetite ao risco era genérica, sem limites quantitativos que descessem até a operação, e as atas do comitê registravam a apresentação dos riscos, mas não a deliberação nem o encaminhamento das ações. O resultado é que a estrutura existia, mas não fechava o ciclo: identificava e reportava, sem decidir e agir de forma rastreável. A correção não exigiu uma nova área, e sim um apetite com limites objetivos e uma disciplina de ata que registrasse decisão e responsável. O caso é genérico e ilustra um padrão recorrente, sem corresponder a qualquer entidade específica.

MERC

Como a MERC pode ajudar

A MERC examina, na auditoria independente e em trabalhos de avaliação de controles e governança, se a estrutura de gerenciamento de riscos de uma entidade regulada existe de fato e produz evidência: se há apetite ao risco definido e comunicado, se as três linhas estão separadas de forma proporcional ao porte, se a auditoria interna tem acesso ao conselho e se a trilha de decisão demonstra que os alertas viraram ação. O trabalho aponta, de forma objetiva, onde a estrutura apenas documenta o risco e onde ela de fato o gerencia, o que importa cada vez mais num ambiente regulatório que responsabiliza o conselho pela posição de risco da organização. Para tratar do seu caso, fale com a equipe pelo contato.

FAQ

Perguntas frequentes

MERC GROUP

PRÓXIMO PASSO

Do requisito ao *teste* que o sustenta.

A MERC e firma de auditoria independente registrada na CVM, especializada em mercado financeiro. Estruturamos o trabalho do diagnostico a evidencia: leitura do requisito, desenho dos testes, trilha de auditoria e o relatorio que sustenta a conclusao. Fale com a equipe pelo canal de contato.

SITE	www.mercgroup.com.br
CONTEÚDO	www.mercgroup.com.br/insights
E-MAIL	contato@mercgroup.com.br
TELEFONE	+55 11 98196 1447

Material técnico de apoio da MERC Group. Conteúdo de caráter informativo, sem constituir oferta de serviços a entidades para as quais a independência seja vedada. Exemplos genéricos, sem referência a instituição específica.