MERCGROUP

APRESENTAÇÃO · APLICAÇÃO PRÁTICA

Controle sem *rastro* não existe.

Como construir trilhas de auditoria e controles internos sob o framework COSO — do desenho à evidência — e por que auditores, reguladores e investidores só aceitam o que está documentado.

SÃO PAULO · BRASIL · 2026

SUMÁRIO EXECUTIVO

O que este material te *entrega*.

- **O framework COSO traduzido para a operação:** os cinco componentes — ambiente de controle, avaliação de riscos, atividades de controle, informação e comunicação, monitoramento — e o que cada um exige na prática.
- **O que é uma trilha de auditoria de verdade:** quem fez, o quê, quando, com que aprovação e com que evidência — nos sistemas, nos processos e nas planilhas críticas.
- **Como dimensionar controles sem burocratizar:** matriz de riscos e controles enxuta, controles-chave versus acessórios e automação onde o volume justifica.
- **Um diagnóstico editável de 12 perguntas** sobre a maturidade dos controles e das trilhas da sua operação.
- **Próximos passos objetivos** com a MERC: desenho e avaliação independente de controles internos com método de auditoria.

Material de aplicação prática elaborado pela MERC Group a partir do artigo "Audit trail e controles internos sob COSO", publicado em 2026 em www.mercgroup.com.br/insights. Este documento tem caráter informativo e não substitui avaliação profissional específica.

Este material não é sobre teoria. É sobre *decisão prática*.

Para o auditor, o regulador e o investidor, vale uma regra dura: o que não está *evidenciado* não aconteceu.

MERCGROUP

CONTEXTO

Do organograma ao *rastro*: o que o COSO exige.

O QUE ACONTECEU

O **COSO** (Committee of Sponsoring Organizations) publica o framework de controles internos mais aceito do mundo — a referência que auditores independentes, reguladores e investidores usam para avaliar se uma organização controla aquilo que reporta.

O modelo tem cinco componentes: **ambiente de controle** (tom da liderança, estrutura, competência), **avaliação de riscos** (o que pode dar errado nos objetivos), **atividades de controle** (aprovações, conciliações, segregação de funções), **informação e comunicação** e **monitoramento** (o controle do controle).

A materialização de tudo isso é a **trilha de auditoria**: o registro que permite reconstruir qualquer número ou decisão — da linha do balanço ao documento de origem, da alteração no sistema ao usuário que a fez, da exceção à aprovação de quem podia aprovar.

A régua subiu com a digitalização: sistemas registram tudo, e a ausência de trilha deixou de ser limitação técnica para virar **escolha de governança**. As NBC TA revisadas para o ambiente digital, os requisitos de reguladores (BCB, CVM) e os padrões de asseguração (ISAE 3402) convergem no mesmo ponto: controle sem evidência não é controle.

O QUE MUDA NA PRÁTICA

Segregação de funções é o controle-mãe. Quem executa não aprova, quem aprova não concilia, quem administra o sistema não opera — em times enxutos, compensações documentadas substituem a segregação plena.

Planilhas críticas entram no perímetro. A planilha que calcula provisão, covenants ou preço é um sistema: precisa de versionamento, controle de acesso e revisão independente — ou migra para ambiente controlado.

Logs precisam ser protegidos e revisados. Trilha que o próprio usuário pode apagar não é trilha; log que ninguém revisa é arquivo morto — a revisão periódica de acessos e alterações é o monitoramento em ação.

Exceção documentada vale mais que regra bonita. O tratamento das exceções — quem aprovou, por quê, com que compensação — é onde auditor e regulador medem a maturidade real do ambiente.

IMPACTO POR PERFIL

Como isso afeta a *sua* companhia.

SECURITIZADORA

A esteira de aquisição de recebíveis é uma cadeia de controles: elegibilidade, formalização, custódia, conciliação — cada elo precisa de trilha que o investidor e o auditor consigam refazer.

FIDC E GESTORA DE FUNDOS

Precificação, enquadramento e ordens têm controles esperados pela CVM e pelo administrador — a evidência de execução é o que sustenta o relatório e evita apontamento.

INSTITUIÇÃO REGULADA BCB

Controles internos são exigência regulamentar formal: estrutura, relatórios periódicos e responsabilização — a trilha alimenta tanto a auditoria quanto os reportes de conformidade.

HOLDING E GRUPOS EMPRESARIAIS

Alçadas, partes relacionadas e rateios intragrupo precisam de matriz de aprovação e rastro — é o que separa gestão centralizada de confusão patrimonial.

EMPRESA EM EXPANSÃO

Investidor institucional testa controles na diligência: fechamento com calendário, conciliações assinadas e sistema com trilha valem pontos diretos no preço e no prazo do deal.

DIAGNÓSTICO RÁPIDO

Onde a sua companhia está *hoje*?

Responda Sim ou Não. Cada "Não" é um ponto de atenção prioritário. Os campos deste formulário são editáveis.

	SIM	NÃO	OBSERVAÇÕES
01. Existe matriz de riscos e controles cobrindo os processos que alimentam as demonstrações financeiras?	☐	☐	
02. Os controles-chave estão identificados e diferenciados dos acessórios?	☐	☐	
03. A segregação de funções está mapeada — e as exceções têm compensações documentadas?	☐	☐	
04. As conciliações relevantes são executadas, revisadas e assinadas com periodicidade definida?	☐	☐	
05. Os sistemas críticos registram trilha de alteração (usuário, data, valor anterior e novo)?	☐	☐	
06. Os logs são protegidos contra alteração e revisados periodicamente por função independente?	☐	☐	
07. As alçadas de aprovação estão formalizadas e refletidas nos sistemas?	☐	☐	
08. As planilhas críticas têm versionamento, controle de acesso e revisão independente?	☐	☐	
09. As exceções e overrides são registrados com justificativa e aprovação de alçada adequada?	☐	☐	
10. Os acessos a sistemas são revisados periodicamente (concessão, mudança de função, desligamento)?	☐	☐	
11. Falhas de controle identificadas viram plano de ação com dono, prazo e evidência de conclusão?	☐	☐	
12. A administração recebe reporte periódico sobre a saúde do ambiente de controles?	☐	☐	

PRÓXIMOS PASSOS

Do diagnóstico à *ação*, com a MERC.

MERC Valuation — valuation.mercgroup.com.br

Avaliação de empresas com metodologia de mercado financeiro: DCF, múltiplos e modelagem avançada, com trilha de premissas auditável.

MERC DF — df.mercgroup.com.br

Elaboração e revisão de demonstrações financeiras em conformidade com CPC e IFRS, prontas para auditoria, credores e investidores.

MERC Lastros — lastros.mercgroup.com.br

Verificação independente de lastros para securitizadoras, FIDCs e operações estruturadas, com evidência e rastreabilidade.

Auditoria & Advisory especializada

Desenho, documentação e avaliação independente de controles internos sob COSO: matriz de riscos e controles, trilhas de auditoria, controles de planilhas e prontidão para auditoria e asseguração (ISAE 3402/NBC TO).

AGENDAR REUNIÃO

Fale com o nosso time: **contato@mercgroup.com.br**

Ou fale diretamente com nossos sócios: **gabriel.carolei@mercgroup.com.br** · **bruno.zamboni@mercgroup.com.br**

FONTES NORMATIVAS

Referências deste material.

NORMAS E REGULAÇÃO BRASILEIRAS

- NBC TA 315 (revisada) — identificação e avaliação de riscos, incluindo ambiente de TI.
- Resolução CMN nº 4.968/2021 — controles internos em instituições autorizadas pelo BCB.
- Resolução CVM nº 21/2021 e normas aplicáveis — controles em participantes do mercado.
- NBC TO 3402 — asseguração de controles em organizações prestadoras de serviços.

REFERÊNCIAS INTERNACIONAIS

- COSO — Internal Control: Integrated Framework (2013).
- ISAE 3402 — Assurance Reports on Controls at a Service Organization (IAASB).
- COBIT — governança de tecnologia (ISACA), referência para controles de TI.

As referências acima indicam o arcabouço normativo aplicável na data de elaboração deste material (julho de 2026) e podem ser alteradas pelos órgãos emissores. A aplicação a casos concretos exige análise específica. MERC Group — Auditoria do Mercado Financeiro Brasileiro · São Paulo · Brasil.