

Praxisnah und entscheidungsorientiert, aber methodisch noch unvollständig

Eine Würdigung der COSO-Veröffentlichung „From Guidance to Action: Exploring Practical Enterprise Risk Management“ (2026) aus Sicht eines entscheidungsorientierten Risikomanagements¹

1. Einordnung

Mit „From Guidance to Action“ veröffentlicht COSO 2026 eine praxisorientierte Handreichung. Wichtig für die Einordnung: Es handelt sich **nicht um ein neues Rahmenwerk**, sondern um eine Konkretisierung des COSO-ERM-Frameworks (2017). COSO versteht das eigene Rahmenwerk dabei ausdrücklich als „Werkzeugkasten“ und will dessen Prinzipien in praktisches Führungsverhalten übersetzen. Die RMA bewertet die Veröffentlichung daher an diesem selbstgesetzten Anspruch, nämlich als Verhaltens- und Umsetzungsleitfaden, und nicht als vollständige Methodenlehre des Risikomanagements.

Die Kernbotschaft trifft einen wunden Punkt vieler Systeme: ERM wird in der Praxis häufig als Pflicht zur Dokumentation von Risiken verstanden, nicht als Grundlage für bessere Entscheidungen. Diesem Befund setzt COSO ein entscheidungsgeführtes, schlankes und in bestehende Planungs-, Steuerungs- und Entscheidungsprozesse eingebettetes ERM entgegen, das entscheidungsrelevante Informationen frühzeitig in strategische und operative Entscheidungen einbringt. Diese Stoßrichtung entspricht unserem Verständnis eines **entscheidungsorientierten Risikomanagements**. Sie ist an die im DACH-Raum geltenden Erwartungen an eine fundierte, nachvollziehbare und risikoadäquate Unternehmensführung, insbesondere an die Anforderungen an die Risikofrüherkennung, die Sorgfaltspflichten von Leitungs- und Aufsichtsorganen sowie eine belastbare Entscheidungsgrundlage bei wesentlichen unternehmerischen Entscheidungen, anschlussfähig. Nationale Regelwerke wie AktG und StaRUG in Deutschland oder vergleichbare Governance- und Sorgfaltspflichten in Österreich und der Schweiz konkretisieren diese Erwartungen unterschiedlich, weisen jedoch in dieselbe Richtung.

Vor diesem Hintergrund fällt unsere Würdigung ausgewogen aus: Wir teilen Anspruch und Richtung der COSO-Veröffentlichung und zeigen zugleich auf, wo aus unserer Sicht der nächste Schritt liegt.

2. Was wir begrüßen

- **Entscheidung vor Dokumentation.** Der konsequente Test „Verändert dieses Arbeitsprodukt eine Entscheidung?“ rückt ERM von der Berichtspflicht zur Entscheidungsvorbereitung. Das ist überfällig und richtig.
- **Strategie- und Chancenorientierung.** Dass jede strategische Wahl eine Risikoposition mit sich bringt und dass ERM früh und kontinuierlich in die Strategiearbeit einbezogen gehört, ist zentral. Ebenso der ausdrückliche Wertbeitrag durch *Schutz und Schaffung*: Die Abkehr vom reinen „Verhindern“ hin zu besseren Chancen-Risiko-Abwägungen entspricht unserem Verständnis moderner Steuerung.
- **Governance als gelebtes Verhalten.** ERM als Betriebssystem in bestehenden Foren, mit klaren Entscheidungsrechten, Eskalationspfaden und konsequenter Nachverfolgung vereinbarter Maßnahmen, statt als paralleler „Risikokalender“. Die Betonung von Ownership im Business und in der wirksamen Prüfung deckt sich mit dem Three-Lines-Gedanken eines abgestimmten Zusammenwirkens von Steuerung und Assurance.

¹ Teile der Recherche und der Formulierung wurden mithilfe von künstlicher Intelligenz durchgeführt. Der finale Text wurde vollständig vom Autorenteam formuliert und auf Richtigkeit geprüft.

- **Kultur und psychologische Sicherheit.** Die konsequente Betonung von Transparenz im Umgang mit Unsicherheit ist eine Stärke der Veröffentlichung: Ohne eine offene Auseinandersetzung über Annahmen, Trade-offs und mögliche Fehlentwicklungen bleibt selbst ein gut konstruiertes System wirkungslos
- **Vielzahl praxisorientierter Beispiele und Umsetzungshilfen.** Ohne Umsetzungshilfen neigen Unternehmen dazu, das Framework als „überdimensioniert“ oder „zu bürokratisch“ abzulehnen. Praxisbeispiele zeigen, wie man die COSO-Prinzipien „proportional“ und ressourcenschonend anwendet.

3. Wo wir weitergehen würden

Unsere Weiterentwicklungsperspektive richtet sich nicht gegen die Richtung, sondern ergänzt sie um die methodische Tiefe, die ein entscheidungsgeführtes ERM mit sich bringt. Da die COSO-Veröffentlichung bewusst auf Verhalten zielt, bleiben einige Bausteine offen, die wir für unverzichtbar halten:

- **Vom Einzelrisiko zum Gesamtrisikoumfang.** Schwere Krisen entstehen selten aus einem Einzelrisiko, sondern aus dem Zusammenwirken mehrerer Risiken. COSO empfiehlt Szenarien und Bandbreiten, bleibt jedoch bei der *methodisch unverbindlichen Risikoaggregation*. Erst die simulationsbasierte Aggregation (Monte Carlo) über die Unternehmensplanung macht den Gesamtrisikoumfang, den Risikokapitalbedarf und bestandsgefährdende Entwicklungen sichtbar. Hier liegt aus unserer Sicht der wichtigste nächste Schritt.
- **Risikoappetit mit der Tragfähigkeit verknüpfen.** Die Veröffentlichung macht Risikoappetit über Schwellen und Trigger hinweg nutzbar. Das ist ein klarer Fortschritt. Wir würden ihn zusätzlich an den aggregierten Gesamtrisikoumfang sowie an Frühwarnindikatoren wie Insolvenzwahrscheinlichkeit, Rating, Covenants, Liquiditätsreserven oder Eigenkapital- bzw. Finanzierungsspielräume koppeln, im Sinne einer wirksamen Früherkennung bestandsgefährdender Entwicklungen und einer belastbaren Beurteilung der finanziellen Risikotragfähigkeit.
- **Die Brücke zur wertorientierten Steuerung.** Damit zwei Strategie- oder Investitionsoptionen risikogerecht verglichen werden können, bedarf es der Übersetzung des aggregierten Risikos in risikogerechte Kapitalkosten sowie in den Unternehmenswert. Diese Verbindung aus Risikoanalyse und Strategiebewertung bleibt in der Veröffentlichung abstrakt.
- **Risk Map-Kritik konsequent zu Ende denken.** COSO kritisiert zu Recht die verbreitete Praxis, Risiken über Eintrittswahrscheinlichkeit und Auswirkung auf einen einzelnen Score zu reduzieren. Wir würden die Konsequenz vollständig ziehen: echte Wahrscheinlichkeitsverteilungen, geeignete Risikomaße (z. B. Value-at-Risk, Expected Shortfall) und, bei dünner Datenlage, strukturierte Expertenschätzungen, Bayes-Updates oder andere transparente Verfahren statt qualitativer Scheingenauigkeit.
- **Nähe zur Steuerung statt enger Compliance-Logik.** Entscheidungsorientiertes ERM entfaltet seine Wirkung dort, wo geplant, budgetiert, investiert und gesteuert wird. Wir würden ERM deshalb stärker mit Controlling, Unternehmensplanung, Treasury und Performance Management verzahnen als mit einer eng verstandenen GRC- oder Compliance-Logik, die leicht defensiv bleibt.

4. Künstliche Intelligenz – Chance mit Augenmaß

Die Veröffentlichung verweist auf die Automatisierung und die KI-gestützte Auswertung von Signalen. Die RMA teilt diese Offenheit. Aus unserer Sicht ist KI besonders wertvoll bei der Risikoidentifikation, der Datenaufbereitung, der Szenarienbildung und der Kommunikation. Die methodischen Kernschritte, insbesondere die planungsbasierte Risikoaggregation, bleiben hingegen Sache nachvollziehbarer, modellbasierter und prüfbarer Verfahren sowie menschlicher Fachexpertise. Wir plädieren für hybride Lösungen, in denen KI unterstützt, ohne die Reproduzierbarkeit und Prüfbarkeit der Ergebnisse zu untergraben.

5. Fazit und Empfehlung

COSO 2026 verbessert die Entscheidungsnähe des ERM spürbar: Strategieanbindung, Trigger, Ownership, Orientierung an den Operating-Rhythmen und eine ernstgemeinte Risikokultur. Als Verhaltens- und Umsetzungsleitfaden ist die Veröffentlichung wertvoll und anschlussfähig. Entscheidungsorientiertes ERM und der COSO-Ansatz sind dabei keine Gegensätze, sondern komplementär: COSO liefert **Betriebssystem und Verhaltensdisziplin**, während die moderne betriebswirtschaftliche Risikoforschung und Praxis die Mess- und Bewertungsmethodik liefern.

Unsere Empfehlung: Die wertvollen Praktiken der Veröffentlichung, um die quantitative, planungsbasierte Kette zu ergänzen: Risiken als Verteilungen beschreiben, planungsbezogen aggregieren, den Risikoappetit an die Tragfähigkeit koppeln und Risiken in Kapitalkosten und Unternehmenswert übersetzen. Erst dann bleibt ERM nicht bei der Umsetzung guter Praktiken stehen, sondern leistet einen nachweisbaren Beitrag zu besseren Entscheidungen unter Unsicherheit.“

Quellen: COSO (2026), *From Guidance to Action: Exploring Practical Enterprise Risk Management*. – COSO (2017), *Enterprise Risk Management: Integrating with Strategy and Performance*. – Aktuelle betriebswirtschaftliche Risikoforschung zur planungsbasierten Risikoaggregation und zur wertorientierten Steuerung.