RMA Risk Management & Rating Association e.V.
Comment (English translation by Michael Jahn-Kozma with use of DeepL)

Practical and decision-oriented, but methodologically incomplete

An assessment of the COSO publication ‘From Guidance to Action: Exploring Practical Enterprise Risk Management’ (2026) from the perspective of decision-oriented risk management

1. Categorization

With “From Guidance to Action”, COSO is publishing a practice-oriented guide in 2026. It is important to note that this is not a new framework, but rather a more concrete elaboration of the COSO ERM Framework (2017). COSO explicitly regards its own framework as a “toolkit” and aims to translate its principles into practical management behaviour. The RMA therefore assesses the publication against this self-imposed criterion – namely as a guide to behaviour and implementation – rather than as a comprehensive methodology for risk management.

The core message hits a sore point for many systems: in practice, ERM is often understood as an obligation to document risks, rather than as a basis for better decision-making. In response to this finding, COSO proposes a decision-driven, streamlined ERM embedded within existing planning, control and decision-making processes, which incorporates decision-relevant information at an early stage into strategic and operational decisions. This approach is consistent with our understanding of decision-oriented risk management. It is consistent with the expectations prevailing in the DACH region regarding sound, transparent and risk-appropriate corporate governance, in particular the requirements for early risk detection, the duties of care incumbent on management and supervisory bodies, and a robust basis for decision-making in the case of significant business decisions. National regulatory frameworks such as the AktG and StaRUG in Germany, or comparable governance and due diligence obligations in Austria and Switzerland, specify these expectations in different ways, but all point in the same direction.

Against this background, our assessment is balanced: we endorse the aims and direction of the COSO publication, whilst at the same time highlighting what we believe to be the next step.

2. What we appreciate:

- **Decision-making before documentation.** The consistent test – ‘Does this deliverable influence a decision?’ – shifts ERM from a reporting obligation to a role in decision-making preparation. This is long overdue and entirely correct**.**
- **Strategy and opportunity orientation.** It is crucial that every strategic choice entails a risk exposure and that ERM should be integrated into strategic work at an early stage and on an ongoing basis. Equally important is the explicit value contribution through protection and creation: the shift away from mere ‘prevention’ towards better opportunity-risk assessments is in line with our understanding of modern governance.
- **Governance as practised behaviour.** ERM as an operating system within existing forums, with clear decision-making powers, escalation paths and consistent follow-up on agreed measures, rather than as a parallel ‘risk calendar’. The emphasis on ownership within the business and in effective auditing aligns with the ‘three lines’ concept of coordinated interaction between governance and assurance**.**

*Please note: parts of the research and drafting were carried out with the aid of artificial intelligence. The final text was checked in full by the team of authors to ensure its accuracy.

– **Culture and psychological safety.** The consistent emphasis on transparency when dealing with uncertainty is one of the publication's strengths: without an open discussion of assumptions, trade-offs and potential pitfalls, even a well-designed system remains ineffective.

– **A wealth of practical examples and implementation guidance.** Without implementation guidance, organisations tend to reject the framework as 'overly complex' or 'too bureaucratic'. Practical examples demonstrate how to apply the COSO principles in a 'proportionate' manner whilst conserving resources

3. What we would like to expand:

Our approach to further development is not intended to run counter to this direction, but rather to complement it with the methodological depth that a decision-led ERM brings. As the COSO publication deliberately focuses on behaviour, some elements remain unaddressed which we consider indispensable:

– **From individual risks to the overall risk profile.** Serious crises rarely arise from a single risk, but rather from the interaction of several risks. COSO recommends scenarios and ranges but remains methodologically non-committal on risk aggregation. Only simulation-based aggregation (Monte Carlo) via corporate planning reveals the overall risk exposure, the risk capital requirement and developments that threaten the company's survival. In our view, this is the most important next step.

– **Linking risk appetite to risk-bearing capacity**. The publication makes risk appetite usable across thresholds and triggers. This is a clear step forward. We would also link it to the aggregated total risk exposure as well as to early-warning indicators such as the probability of insolvency, credit ratings, covenants, liquidity reserves or equity and financing headroom, with a view to effectively identifying developments that threaten the company's continued existence at an early stage and making a robust assessment of its financial risk-bearing capacity.

– **The link to value-based management**. In order to compare two strategic or investment options on a risk-adjusted basis, the aggregated risk must be translated into risk-adjusted costs of capital and into enterprise value. This link between risk analysis and strategy evaluation remains abstract in the publication.

– **Thinking through the criticism of the Heat Map to its logical conclusion.** COSO is right to criticise the widespread practice of reducing risks to a single score based on probability of occurrence and impact. We would take this logic to its full conclusion: genuine probability distributions, appropriate risk measures (e.g. Value-at-Risk, Expected Shortfall) and, where data is scarce, structured expert estimates, Bayesian updates or other transparent methods rather than qualitative pseudo-precision.

– **Closer alignment with management rather than a narrow compliance-based approach.** Decision-oriented ERM is most effective where planning, budgeting, investment and management take place. We would therefore integrate ERM more closely with management accounting, corporate planning, treasury and performance management than with a narrowly defined GRC or compliance framework, which tends to remain defensive.

4. Artificial Intelligence– Opportunity with sense of proportion

The publication refers to automation and AI-supported signal analysis. The RMA shares this openness. In our view, AI is particularly valuable for risk identification, data preparation, scenario building and communication. The core methodological steps, however – in particular planning-based risk aggregation – remain the preserve of transparent, model-based and verifiable procedures, as well as human expertise. We advocate hybrid solutions in which AI provides support without undermining the reproducibility and verifiability of the results.

*Please note: parts of the research and drafting were carried out with the aid of artificial intelligence. The final text was checked in full by the team of authors to ensure its accuracy.

5. Conclusion and Recommendation

COSO 2026 significantly improves the alignment of ERM with decision-making: strategic alignment, triggers, ownership, alignment with operational rhythms, and a genuine risk culture. As a guide to behaviour and implementation, the publication is valuable and adaptable. Decision-oriented ERM and the COSO approach are not opposites, but complementary: COSO provides the operating system and behavioural discipline, whilst modern business risk research and practice provide the measurement and assessment methodology.

Our recommendation: to use the valuable practices outlined in the publication to complement the quantitative, planning-based framework: describe risks as distributions, aggregate them in relation to planning, link risk appetite to the organisation's capacity to absorb risk, and translate risks into cost of capital and enterprise value. Only then will ERM go beyond merely implementing good practices and make a demonstrable contribution to better decision-making under uncertainty.

References: *COSO (2026), From Guidance to Action: Exploring Practical Enterprise Risk Management. – COSO (2017), Enterprise Risk Management: Integrating with Strategy and Performance - Recent business risk research on planning-based risk aggregation and value-based management.*

*Please note: parts of the research and drafting were carried out with the aid of artificial intelligence. The final text was checked in full by the team of authors to ensure its accuracy.