STEFAN HUNZIKER

DAS NEUE COSO ERM FRAMEWORK AUF DEM PRÜFSTAND

Wie viel Innovation und Praxisanleitung steckt in der neusten Version des Risk-Management-Standards?

Vor Kurzem ist das Update «COSO Enterprise Risk Management – Integrating with Strategy and Performance» erschienen – 13 Jahre nach dem ersten Release des COSO ERM Framework. Es soll einen hohen Strategiebezug aufweisen und in die Geschäftsprozesse integriert sein. Doch hält der Titel des neuen Framework, was er verspricht? Der Beitrag beleuchtet diese Frage kritisch.

1. EINLEITUNG

Seit dem ersten Release des COSO ERM Framework 2004, des *Enterprise Risk Management (ERM)* Framework des *Committee of Sponsoring Organizations of the Treadway Commission (COSO),* sind 14 ereignisreiche Jahre vergangen, die aus einer Risikoperspektive insbesondere durch die Finanzkrise 2007–2008 geprägt waren. Risk Management hat durch Letztere zweifelsohne Auftrieb in der Führungsebene erhalten; der sogenannte «schwarze Schwan» wurde real. Vielen Unternehmen wurde vor Augen geführt, dass Risk Management in der Unternehmensführung unverzichtbar ist, stellte sie aber gleichzeitig vor die Herausforderung einer nutzenstiftenden Umsetzung. Insbesondere die zentrale Frage nach der Integration in Führungs- und Entscheidungsprozesse scheint für viele Unternehmen bis heute nur schwer lösbar zu sein. Das COSO erkannte diese praktischen Probleme und ergriff mit der Ankündigung für ein Update 2014 die Chance, diesbezüglich mehr Klarheit zu schaffen.

Das Update, das von *PwC* unter der Leitung des COSO Board entwickelt wurde, hebt im Titel des Rahmenwerks folgerichtig die Bedeutung der Abhängigkeiten von Risk Management, strategischer Planung und Unternehmenserfolg hervor. Zusätzlich soll der Einbettung von Risk Management in die gesamte Organisation stärker Rechnung getragen werden. Bei der Überarbeitung des Rahmenwerks erhielt PwC im Rahmen der Vernehmlassungsphase viele Anregungen von diversen Anspruchsgruppen, dem COSO Board sowie dessen Advisory Council.

Im Rahmen des vorliegenden Beitrags muss geklärt werden, woran das Update gemessen und gespiegelt werden soll. Es ist nicht das Ziel, einen Vergleich mit anderen Standards und Normen vorzunehmen oder schwerpunktmässig Differenzen zur Erstpublikation des COSO ERM aus dem Jahr 2004 herauszuarbeiten. Aus praxisorientierter Sicht scheint der Vergleich mit dem modernen Verständnis von Risk Management primär relevant: Risk Management wird als integrativer Bestandteil guter Unternehmensführung verstanden und unterstützt entsprechend Entscheidungsprozesse.

STEFAN HUNZIKER,
PROF. DR. OEC. HSG,
INSTITUT FÜR FINANZDIENSTLEISTUNGEN ZUG (IFZ),
HOCHSCHULE LUZERN, ZUG

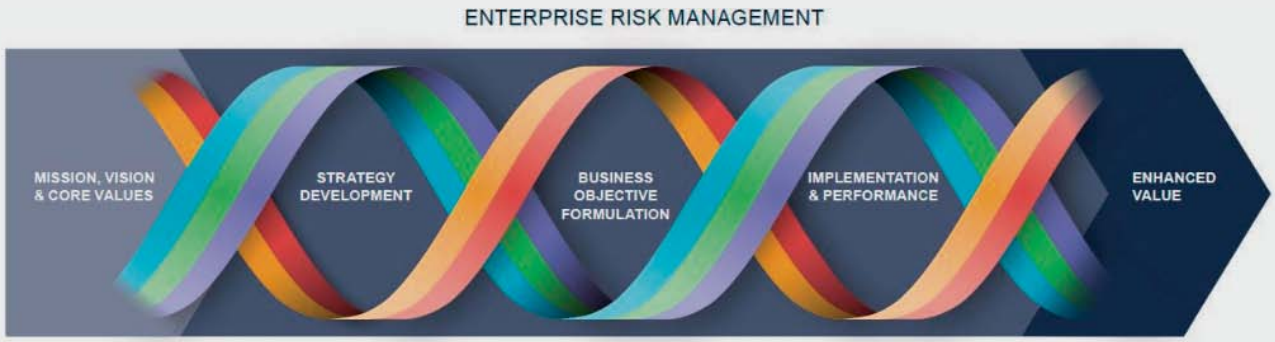
2. STRUKTUR UND FOKUS

Wer die Zeit dafür aufgebracht hat, das Dokument ganzheitlich zu studieren, wird vieles aus der Vorgängerversion von 2004 wiedererkennen, aber auch signifikante Unterschiede ausmachen. Insbesondere die Dokumentenstruktur sowie die grafische Aufmachung wurden stark überarbeitet.

2.1 Titel, Struktur und Grafiken. Vorweg: Der interessierte Leser benötigt viel Geduld beim Durchlesen des gesamten Hauptdokuments. Das finale Framework ist mit 110 Seiten (29 Seiten Einführung, 81 Seiten Rahmenwerk) umfassend und ähnelt in bestimmten Passagen mehr einem Lehrbuch mit vielen Definitionen als einer kurz gefassten, praxisorientierten Leitlinie. Allerdings muss positiv hervorgehoben werden, dass klare Fortschritte im Vergleich zur Draft-Version erkennbar sind, v. a. bezüglich Struktur, Länge, Kapitelbezeichnungen und konkreteren Beispielen in einigen Prinzipien (z. B. zum Risikoappetit und zur Portfoliosicht von Risiken). Es zeigt sich, dass die Kommentare renommierter Risk-Management-Vertreter im Vernehmlassungsprozess nicht ohne Wirkung geblieben sind.

Als Erstes fällt der neue Titel des Framework auf: «Enterprise Risk Management – Integrating with Strategy and Performance»; er betont den Bezug zur Strategie und zum Un-

Abbildung 1: **COSO ERM 2017 IN NEUER GRAFISCHER AUFMACHUNG** [1]



ternehmenserfolg und grenzt damit auch klarer von der Thematik der internen Kontrolle ab. Weiter wurde die Dokumentenstruktur stark überarbeitet, auf den altbekannten COSO-Würfel wurde verzichtet. Das Update enthält nur noch fünf Komponenten, denen insgesamt 20 Prinzipien zugeordnet werden. Anstelle des Würfels steht nun eine Grafik, die das COSO ERM 2017 in seiner Grundidee repräsentiert *(Abbildung 1)*.

Grundsätzlich ist die Abwendung vom COSO-Würfel, der Risk Management sehr stark isoliert dargestellt hat, sehr zu begrüssen. Die neue Abbildung zeigt einen deutlich stärkeren Bezug zum Geschäftsmodell und macht deutlich, dass Risk Management ein Bestandteil der Unternehmensentwicklung und -führung sein muss. Dies wird auch durch das gesamte Dokument immer wieder betont und mit neuen Grafiken unterlegt, die den Bezug zwischen Strategie, Erfolg, Risikoappetit und Risikokapazität aufzeigen. Etwas schwerfällig gestaltet sich allerdings das Lesen des Rahmenwerks. Obwohl die Grundstruktur des Dokuments eigentlich klar erscheint, werden bestimmte Aussagen häufig wiederholt. Ein roter Faden, an dem sich der Praktiker bei der Umsetzung orientieren könnte, ist schwer zu erkennen. Obwohl das COSO ERM 2017 konzeptionell darum bemüht ist, Risk Management als integratives Instrument der Unternehmensführung zu positionieren, zeigt sich das noch zu wenig in der gewählten Sprache. Diese ist immer noch zu technisch und auf die Profession des Risk Manager fokussiert. In der Praxis besteht die Herausforderung gerade darin, die «sprachliche Brücke» zwischen dem Risk Manager und dem Business zu überwinden.

> *«Das COSO ERM 2017 präsentiert einen klaren Business Case, wie Risk Management Werte schafft, wenn es in den Strategieprozess und die Erfolgssteuerung eines Unternehmens integriert wird.»*

2.2 Starker Management- und Corporate-Governance-Fokus. In Bezug auf die inhaltliche Ausrichtung fällt auf, dass ein grosser Teil des gesamten Framework auf eine angemessene Unternehmensführung und auf allgemeine Managementprinzipien fokussiert. Grundsätzlich müsste das COSO ERM also auch mit in der Schweiz relevanten Corporate-Governance-Richtlinien wie dem «Swiss Code of Best Practice for Corporate Governance» verglichen werden. *Abbildung 2* zeigt überblicksartig die thematischen Schwerpunkte des 81-seitigen, revidierten Framework.

Zusammenfassend ist festzuhalten, dass insbesondere die Komponente «Performance», die knapp ein Drittel des Rahmenwerks ausmacht, Kernthemen des Risk Management aufgreift. Alle anderen Komponenten stellen zwar mehr oder weniger Bezüge zum Risk Management her, fokussieren aber primär aufs Thema der guten Unternehmensführung. Nachfolgend werden ausgewählte Aspekte aus dem Update 2017 diskutiert, die hinsichtlich der Umsetzung eines modernen Risk Management kritisch sein können.

3. INTEGRATION IN ENTSCHEIDUNGSPROZESSE

Eine der prominentesten Botschaften wird unter dem Titel «Integrating Enterprise Risk Management» auf drei Seiten des Rahmenwerks angesprochen. Das COSO ERM 2017 präsentiert einen klaren Business Case, wie Risk Management Werte schafft, wenn es in den Strategieprozess und die Erfolgssteuerung eines Unternehmens integriert wird. Stellvertretend dafür steht die Aussage «When making [...] decisions, management and the board must continually navigate a dynamic business context, which requires integration enterprise risk management thinking into all aspects of the entity, at all times.» [2] Grundsätzlich ist die Forderung vom COSO nach einer Integration von Risk Management in alle Entscheidungsprozesse der Unternehmung sehr zu begrüssen. Im Rahmenwerk wird wiederholt angemerkt, dass Risikoüberlegungen in Form von Szenarioanalysen in die Strate-

Abbildung 2: **THEMATISCHE SCHWERPUNKTE DES COSO ERM 2017**

Komponenten	Prinzipien	Inhaltlicher Fokus
Governance and Culture	1. Excercises Board Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	*18 Seiten von 81 (22 %)* Starker Bezug zu generellen Prinzipien guter Unternehmensführung und Kultur. Der Bezug zu Risk Management wird hergestellt, wenn auch eher knapp.
Strategy and Objective Setting	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	*20 Seiten von 81 (25 %)* Ausser Prinzip 7 primär eher theoretische Auseinandersetzung mit dem Geschäftsumfeld, der Strategie sowie dem Zielfestlegungsprozess.
Performance	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View	*23 Seiten von 81 (28 %)* Kernkomponente zum Risk Management inkl. der Verbindung von Risk Management zur Strategie, zur Zielfestlegung und zum Erfolg.
Review and Revision	15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues Improvement in Enterprise Risk Management	*8 Seiten von 81 (10 %)* Prinzipien 16 und 17 fokussieren auf Risk Management bzw. den Verbesserungsprozess. Prinzip 15 bezieht sich auf die Identifikation von Veränderungen (extern und intern).
Information, Communication and Reporting	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance	*12 Seiten von 81 (15 %)* Prinzip 18 bezieht sich relativ allgemein auf IT- und Informationssysteme im Unternehmen. Prinzipien 19 und 20 adressieren die risikobezogene Berichterstattung.

gieentwicklung und -umsetzung eingebettet werden sollen. Alternative Strategien weisen unterschiedliche Risiken auf, und diese Informationen müssen dem Management vorliegen, damit es sich für oder gegen eine strategische Option entscheiden kann. Weiter impliziert dieses Statement auch, dass Risk Management mehr als eine periodische Neubeurteilung eines Risikoinventars beinhaltet und fortlaufend im Tagesgeschäft umgesetzt werden muss («... all aspects of the entity, at all times»).

Allerdings lassen sich zu dieser positiven Grundforderung in den Details im Framework erhebliche Probleme und Inkonsistenzen aufdecken. Obwohl Risk Management sehr zentral mit Entscheidungsqualität in Verbindung gebracht wird, liefert das COSO keine Anhaltspunkte in Form eines der 20 Prinzipien mit konkreten Beispielen, wie Entscheidungen unter Unsicherheit getroffen werden sollen. Weiter widerspricht die später im Rahmenwerk vorzufindende Diskussion über den Risikobegriff und die Risikobewertung obiger Forderung. Das COSO stellt klar das negative Risiko (was kann schiefgehen?) in den Vordergrund. Dies kann zu einer erheblichen Überbewertung des unternehmerischen Gesamtrisikos führen, wenn Chancen nicht gleichermassen

Abbildung 3: **RISK MAP ALS «PROBLEMATISCHES» INSTRUMENT ZUR BEURTEILUNG VON RISIKEN** [4]

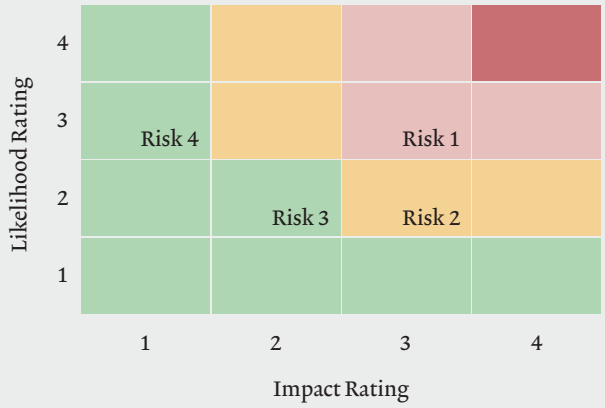
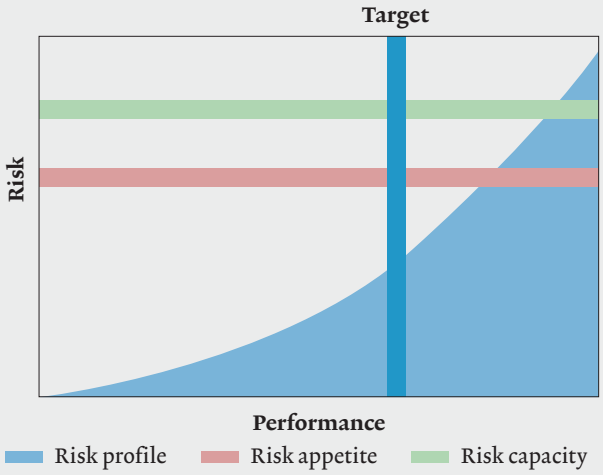


Abbildung 4: **ZUSAMMENHANG ZWISCHEN RISIKOPROFIL, RISIKOKAPAZITÄT UND RISIKOAPPETIT** [5]



berücksichtigt werden. Gerade in der Bewertung strategischer Alternativen müsste das COSO demnach dafür plädieren, einen konsistenten Bewertungsansatz für alle Konsequenzen anzuwenden – für die guten wie die schlechten. Zusammenfassend wird den Entscheidungsträgern kein genügendes Hilfsmittel an die Hand gegeben, wie Risk Management im Alltag Entscheidungsprozesse unterstützt und damit Risiko-Ertrags-Alternativen besser zu beurteilen vermag.

4. RISIKOBEURTEILUNG UND RISIKOAPPETIT

Die Risikobeurteilung stellt zweifelsohne eine der erfolgskritischen Kernthematiken im Risk Management dar. Sie gibt Auskunft über die momentane Risiko- und Chancenlage des Unternehmens und wird oft dem Risikoappetit gegenübergestellt. Allerdings zeigt sich in der Praxis die Schwierigkeit, einen handlungsanweisenden Appetit zu definieren und für Entscheidungen zu nutzen. Schafft das COSO ERM 2017 hierzu Klarheit und Fortschritt?

4.1 Risikobeurteilung: Nicht viel Neues. Irritierend im gesamten Framework ist die inkonsistente bzw. zu einseitige Verwendung des Risikobegriffs. Obwohl das COSO klar definiert, dass mit einem Risiko negative (risks) oder positive (opportunities) Konsequenzen für die Strategie bzw. die Unternehmensziele gemeint sind, wird der Fokus in den einzelnen Prinzipien stark auf das Bewirtschaften der «risks» gelegt. Ein deutlich besserer und modernerer Ansatz wäre es, spezifischer in Unsicherheiten oder Wertebereichen zu denken. In der Realität sind Risiken und Chancen selten einzelne Punktschätzungen, sondern stellen einen «Bereich von Unsicherheit» dar, der realistischerweise verschiedene positive und negative Szenarien mit unterschiedlichen Eintrittswahrscheinlichkeiten enthält. Auch die konsequente Orientierung der Risikobewertung an den Unternehmenszielen fehlt im Framework; die unabhängige Risikobetrachtung steht immer noch zu stark im Vordergrund. Insofern werden die einzelnen Prinzipien zur Risikobeurteilung nicht vollumfänglich dem Titel-Versprechen des neuen Framework gerecht.

Erfreulich ist, dass das COSO im Bereich der Risikobeurteilung neu auch Erkenntnisse aus der Wirtschaftspsychologie und der Verhaltensforschung (cognitive biases) berücksichtigt, die allerdings schon jahrzehntelang vorliegen und bereits in der ersten Version hätten aufgenommen werden müssen. Beispielsweise weist das COSO darauf hin, dass die Risikobeurteilung stets auch von der Risikoeinstellung (Risikokultur) abhängt, und erläutert, dass es ein Spektrum von sehr risikoaversen bis sehr risikoaggressiven Unternehmen gibt. Auch die Erkenntnis, dass Unternehmen oder Individuen in Verlustsituationen mehr Risiko auf sich nehmen als

> *«Positiv zu werten ist im Vergleich zur früheren Version des COSO ERM die ausführlichere, anschaulichere Diskussion zum Risikoappetit und dessen Verbindung zum Unternehmenswert und zur Risikokapazität.»*

in Gewinnsituationen, wird mit einem Beispiel unterlegt. Allerdings erhält der Leser den Eindruck, dass das COSO mit dem kurzen Abschnitt «Bias in Assessment» lediglich zeigen will, dass es sich der Relevanz kognitiver Fehlleistungen im Risk Management bewusst ist. Tatsächlich Eingang in die konkrete Umsetzung der Risikobeurteilung finden diese Überlegungen kaum.

Im Zusammenhang mit der Risikobeurteilung taucht auch wieder die altbekannte Risk Map (heat map) auf, die impliziert, dass Risiken einmalig mit Eintrittswahrscheinlichkeit und Schadensausmass zu beurteilen sind (*Abbildung 3*). Ein besserer Ansatz bestünde darin, in Szenarien zu denken. Die Risk Map ist leider nach wie vor ein Standard-

Abbildung 5: **GESAMTBEURTEILUNG COSO ERM 2017**

Themenaspekt	Beurteilung
Struktur und Sprache	+ stärkerer Business-Bezug, auch in den Grafiken + nachvollziehbarer Kapitelaufbau + Verabschiedung vom COSO-Würfel – teilweise zu theoretisch, viele Definitionen – zu langatmig und wiederholend – zu viel technischer Jargon – in sich nicht konsistent (Widersprüche Titel, Ziele und Prinzipien)
Risk Management als Business Case	+ Titel des Framework + Integrationsgedanke steht im Vordergrund + Business Case postuliert den Wert von ERM + ERM ist an den Unternehmenszielen ausgerichtet (stärkere Betonung als im COSO 2004) + Integration von ERM in alle Entscheidungsprozesse + Integration auf allen Ebenen der Organisation – in der praktischen Umsetzung zu wenig konkret – kein konsistentes Ausrichten der einzelnen Prinzipien an der Integrationsforderung – kein Prinzip befasst sich mit ERM und Entscheidungsprozessen
Kernprozesse von Risk Management	+ Risikodefinition umfasst auch positive Abweichungen (Chancen) + Risiken können verschieden identifiziert werden, auch im Umfeld + Risiko als Unsicherheit in Bezug auf die Zielerreichung + Erwähnung kognitiver Verzerrungen – zu starke Orientierung am negativen Risiko (im Widerspruch zur Risikodefinition) – keine verschiedenen Risikoszenarien pro Risiko – Risk Map als Instrument zur Risikobeurteilung – Risikoappetit kaum umsetzbar, zu theoretisch
Risikokultur	+ Risikokultur erstmals ausführlich diskutiert + Einfluss der Risikokultur (menschliches Verhalten) auf Entscheidungen und Beurteilungen erwähnt – zu theoretisch – zu wenig praktische Anleitung
Überprüfung der Wirksamkeit von Risk Management	– keine Anleitung, wie die Effektivität von ERM überprüft werden kann

instrument im Risk Management, das sich hartnäckig in der Praxis hält [3]. Diesbezüglich hat das COSO ERM 2017 die Chance verpasst, sich endlich von der mit vielen bekannten Problemen behafteten Risikolandkarte loszusagen. Letztere steht im Widerspruch zum Hauptanliegen von COSO, der Verknüpfung von Risiken und Chancen mit den Unternehmenszielen und der Integration in Entscheidungsprozesse.

Insgesamt kann festgehalten werden, dass das COSO ERM 2017 keine konsistente Anleitung für die Praxis liefert, wie die Risikobewertung vor dem Hintergrund der (strategischen) Zielerreichung umgesetzt werden kann.

4.2 Die Krux mit dem Risikoappetit. Der Risikoappetit ist eine konkrete Aussage darüber, welche Arten von Risiken ein Unternehmen in welchem Ausmass und zu welcher Eintrittswahrscheinlichkeit bewusst akzeptiert, um die Unternehmensziele erreichen zu können. Die Nutzenaspekte eines präzis definierten Risikoappetits sind zumindest theoretisch klar: Entscheide können vor dem Hintergrund einer Risiko- und Chancenabwägung getroffen werden. So kann der Risikoappetit etwa hinzugezogen werden, wenn ein Unternehmen durch einen anstehenden strategischen Entscheid wissen möchte, ob dem Unternehmen zu viel Risiko hinzugefügt würde. Der Risikoappetit stellt idealerweise auch eine Leitlinie für die strategische Planung dar, indem die Planung an der maximal möglichen Risikokapazität reflektiert wird. So wird klar, dass Risiko per se nicht zu vermeiden ist, aber eine spezifische Obergrenze eingehalten werden muss.

Grundsätzlich positiv zu werten ist im Vergleich zur früheren Version des COSO ERM die ausführlichere und etwas

anschaulichere Diskussion zum Risikoappetit und dessen Verbindung zum Unternehmenswert und zur Risikokapazität. *Abbildung 4* zeigt den vom COSO postulierten Zusammenhang zwischen Risikoappetit, Risikokapazität und Unternehmenserfolg. In der praktischen Umsetzung sind jedoch einige Herausforderungen zu meistern, die nachfolgend kurz skizziert werden.

Erstens definiert das COSO ERM 2017 den Risikoappetit primär über das Schadenpotenzial und vernachlässigt die Eintrittswahrscheinlichkeit, was dem Risikobegriff grundsätzlich widerspricht. Zweitens impliziert die Gegenüberstellung des Risikoappetits mit dem Risikoprofil eine Risikoaggregation, d. h. eine Verdichtung aller Risiken zu einer übergeordneten Risikoverteilung. Wie eine solche Aggregation in der Praxis zu erfolgen hat, wird nicht näher erläutert. Ähnliches gilt für die Unternehmensziele (targets), wovon es wohl mehrere gibt, die unterschiedliche Risiko- und Chancengefüge aufweisen. Drittens wird nicht ganz klar, welche Chance (opportunities) mit dem eingegangenen Risiko verbunden ist. Viertens ist gerade in der Praxis die Definition eines quantifizierten Risikoappetits sehr schwierig, weshalb konkrete Beispiele hilfreich wären. Schliesslich definiert das COSO zwar den Begriff «Risikokapazität» als maximales Risiko, das ein Unternehmen noch absorbieren kann. Allerdings bleibt eine konkrete Anleitung aus, wie vor allem Nichtfinanzunternehmen diese Kapazität berechnen bzw. bestimmen können.

Alternativ zu einer Berechnung des Risikoappetits bietet das COSO ERM 2017 Unternehmen auch die Option an, sehr einfache, qualitative Aussagen zu formulieren. Beispiele wie «Wir weisen bezüglich Geschäftsfeld X einen geringen Risikoappetit auf» sind für die vom COSO ERM postulierte Integration in Entscheidungsprozesse allerdings nutzlos; sie lassen sich nicht in konkrete Handlungsempfehlungen ummünzen.

Korrekterweise greift das COSO ERM 2017 die Problematik auf, wie ein strategisches Risikoappetit-Statement auf die einzelnen operativen Geschäftsziele heruntergebrochen werden kann, damit Entscheidungsträger ihre Entscheidungen am Risikoappetit spiegeln können. Das Rahmenwerk schuldet dem Praktiker aber eine Anleitung, wie die Verbindung zwischen Risikoappetit und operativen Entscheidungsprozessen umzusetzen ist. Die im Risikoappetit formulierten Aussagen vom Aufsichtsorgan und der Geschäftsleitung müssen sich auf das operative Geschäft übertragen lassen, ansonsten bleibt der Risikoappetit eine wirkungslose Worthülse [6]. Schliesslich relativiert das COSO ERM selbst die Entscheidungskraft des Risikoappetits. Es könne sich lohnen, den Risikoappetit auch zu überschreiten, falls der subjektiv wahrgenommene Nutzen dadurch grösser sei, als innerhalb des Risikoappetits zu bleiben. Auch hier lässt sich kein konkretes Beispiel im Rahmenwerk finden.

5. ZUSAMMENFASSENDE BEURTEILUNG

Die umfassendste Beurteilung würden zweifelsohne Unternehmen abgeben können, die das COSO ERM selbst ganzheitlich umgesetzt haben. Allerdings gibt es bis dato keine verlässlichen Studien, ob das COSO ERM (2004 und 2017) in der Realität tatsächlich funktioniert, d. h. Unternehmenswerte schafft. Es ist erstaunlich, dass 14 Jahre nach der Erstveröffentlichung des COSO ERM noch keine Erkenntnisse von Unternehmen vorliegen, die das Rahmenwerk als Ganzes erfolgreich umgesetzt haben.

In *Abbildung 5* wird das COSO ERM 2017 im Sinne einer Gesamtbeurteilung kritisch gewürdigt.

Wird das COSO ERM 2017 dem aktuellen Wissensstand zum modernen Risk Management gegenübergestellt, werden die Bemühungen vom COSO sichtbar, sich den Best Practices anzunähern. Bereits das Aufgreifen menschlichen Fehlverhaltens in Entscheidungssituationen, die Ausrichtung von ERM an der Strategie, die Forderung der Integration in Führungs- und Kernprozesse sowie die stärker am Business ausgerichtete Logik des gesamten Framework bestätigen dies klar. Zudem muss die Beurteilung auch stets vor dem Hintergrund erfolgen, dass das COSO ERM 2017 den Konsens sehr vieler unterschiedlicher Meinungsträger widerspiegeln muss und somit höchstens für den «Durchschnitt» gelten kann. Innovationen, in denen sich die Praxis noch nicht wiedererkennt, finden deshalb nur schwer Eingang in Rahmenwerke.

6. FAZIT

Die Grundidee des COSO ERM 2017, Risk Management als integrativen Bestandteil guter Unternehmensführung (noch stärker) zu positionieren, ist sehr zu begrüssen. Das COSO ERM 2017 liefert dem Praktiker zweifelsfrei ein gutes Argumentarium gegenüber der Unternehmensführung, das eigene Risk Management zu überarbeiten und damit die noch oft vorhandene Hürde zur Verbindung von Risk Management und Entscheidungsprozessen zu überwinden. Allerdings bleibt die praktische Umsetzung dieser Integrationsforderung auch nach dem Durcharbeiten der 20 Prinzipien diffus. Kernthemen wie Risikoidentifikation und -quantifizierung, Risikoaggregation und Risikoappetit enthalten relativ wenig Innovation und praktische Anleitung. Der Kernforderung nach der Integration in Entscheidungsprozesse wird leider in keinem der Prinzipien angemessen Rechnung getragen. ■

Anmerkungen: 1) Vgl. COSO (2017), Enterprise Risk Management – Integrating with Strategy and Performance, Jersey City, NJ: AICPA, S. 21. **2)** COSO (2017), Enterprise Risk Management – Integrating with Strategy and Performance, Jersey City, NJ: AICPA, S. 17. **3)** Vgl. zu einer ausführlichen Diskussion der Probleme von Risk Maps Hunziker, S. (2018), Erfolgskriterien von Enterprise Risk Management in der praktischen Umsetzung, in: Hunziker, S., Meissner, J. O. (Hrsg.), Ganzheitliches Chancen- und Risikomanagement, Springer Gabler, S. 15 ff. **4)** Vgl. COSO (2017), Enterprise Risk Management – Integrating with Strategy and Performance, Jersey City, NJ: AICPA, S. 77. **5)** Vgl. COSO (2017), Enterprise Risk Management – Integrating with Strategy and Performance, Jersey City, NJ: AICPA, S. 49. **6)** Vgl. Hunziker, S. (2018), Erfolgskriterien von Enterprise Risk Management in der praktischen Umsetzung, in: Hunziker, S., Meissner, J. O. (Hrsg.), Ganzheitliches Chancen- und Risikomanagement, Springer Gabler, S. 9.