Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Wirtschaft

CARF Luzern 2018

Controlling.Accounting.Risiko.Finanzen.

Konferenzband

Konferenz Homepage: www.hslu.ch/carf

Risk Governance and Culture als Komponente im neuen COSO Enterprise Risk Management Framework: Konstitutionelles Rahmenwerk für ein wirksames ESG-Risikomanagement?

Extended Abstract

Michael Mies, M.Sc.
Universität Siegen, Doktorand an der Juniorprofessur für Risk Governance, 57072 Siegen, E-Mail: michael.mies@uni-siegen.de

Prof. Dr. Michael Torben Menk
Universität Siegen, Juniorprofessur für Risk Governance, 57072 Siegen, E-Mail: menk@bank.wiwi.uni-siegen.de

Florian Neitzert, B. Sc.
Universität Siegen, Graduate School – Fast-Track PhD, 57072 Siegen, E-Mail: florian.neitzert@uni-siegen.de

Abstract
Durch Novellierung des Frameworks Enterprise Risk Management: Aligning Risk with Strategy and Performance verfolgt das Committee of Sponsoring Organizations of the Treadway Commission (COSO) einen Paradigmenwechsel hin zu einer stärkeren Strategie-Orientierung. Die hinzugefügte neue Komponente Risk Governance and Culture rückt als konstitutives Rahmenwerk für die integrierte Governance der ganzheitlichen Risikomanagementfunktion in den Fokus. Insbesondere vor dem Hintergrund steigender Relevanz von Environmental, Social und Governance spezifischen Risiken im Zuge verschärfter Offenlegungsanforderungen der Gesetzgeber ist es für die Unternehmenspraxis sinnvoll sich frühzeitig mit der Aufsetzung entsprechender Governance-Mechanismen zu beschäftigen.

1 Einleitung

Das 2004 vom Committee of Sponsoring Organizations of the Treadway Commission (COSO) veröffentlichte Rahmenwerk "Enterprise Risk Management - Integrated Framework" hat im letzten Jahrzehnt eine breite Akzeptanz in der Unternehmenspraxis (COSO, 2017) und in der betriebswirtschaftlichen Forschung gewonnen (Beasley, Clune, & Hermanson, 2005, p. 522 f.). Durch Novellierung des Frameworks "Enterprise Risk Management: Integrating with Strategy and Performance" reagiert das COSO auf veränderte Anforderungen an das Risikomanagement: Steigende Komplexität, neu auftretende Risiken und ein verbessertes Verständnis von Aufsichtsorganen und Management haben eine Anpassung des bisherigen Frameworks erforderlich gemacht. Durch den gewählten Paradigmenwechsel hin zu einer stärkeren Strategieorientierung soll die Risikomanagementfunktion verstärkt in den Strategie- und den unternehmensweite Leistungserstellungsprozess eingebunden werden (COSO, 2017, Foreword).

Die hinzugefügte neue Komponente Risk Governance and Culture rückt als konstitutives Rahmenwerk für die integrierte Governance der ganzheitlichen Risikomanagementfunktion in den Fokus der Betrachtung (COSO, 2016, p. 22). Erste empirische Erkenntnisse von Schweizer Unternehmen konstatieren eine hohe Relevanz von Integrität und Ethik, jedoch Schwächen in der Dokumentation von Risk Governance Elementen (Hunziker & Balmer, 2018, p. 89 ff.; Hunziker, Balmer, & Schellenberg, 2016, p. 7 f.).

Insbesondere vor dem Hintergrund steigender Relevanz von Environmental, Social und Governance spezifischen Risiken im Zuge verschärfter Offenlegungsanforderungen der Gesetzgeber, ist es für die Unternehmenspraxis sinnvoll sich frühzeitig mit der Aufsetzung entsprechender Governance-Mechanismen zu beschäftigen (WBCSD, 2017, p. 38). Eine erste Indikation zur Aufsetzung entsprechender Systeme liefert die gemeinsam vom COSO und WBCSD herausgegebene Vorentwurfsfassung "Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks" (COSO & WBCSD, 2018). Zielsetzung dieses Beitrages soll es sein, eine Abgrenzung der Komponente Risk Governance and Culture vorzunehmen und Anforderungen an die Governance zur Mitigation von Environmental, Social und Governance bezogenen Risiken aufzuzeigen.

2 Vom Integrated Framework zur Aligning Risk with Strategy and Performance

Im Zuge der verschärften Anforderungen an ein Internes Kontrollsystem durch den Sarbanes-Oxley-Act 2002 hat sich das COSO Internal Control - Integrated Framework als massgebliches Rahmenwerk zur Implementierung und Prüfung der Effektivität des IKS etabliert. Als Ergänzung des ICS Frameworks wurde in 2004 das bisherige COSO II Enterprise Risk Management Framework als Ergänzung veröffentlicht, um eine Bewertung und Verbesserung des unternehmensweiten Risikomanagements zu ermöglichen (COSO, 2004, Foreword).

Ausgehend von der Mission und Vision wird im ERM Rahmenwerk die Strategie eines Unternehmens in die Kategorien strategische Ziele, betriebliche Ziele, Berichterstattung und Compliance mit Gesetzen und Vorschriften abgeleitet. Das ERM basiert auf acht interaktiven Kernkomponenten, die sich an den heruntergebrochenen Unternehmenszielen orientieren (COSO, 2004, p. 3 f):

- Internal Environment,
- Objective Setting,
- Event Identification,
- Risk Assessment,
- Risk Response,
- Control Activities,
- Information & Communication und Monitoring.

Zusammenfassend lässt sich das COSO ERM in Form eines Würfels darstellen.

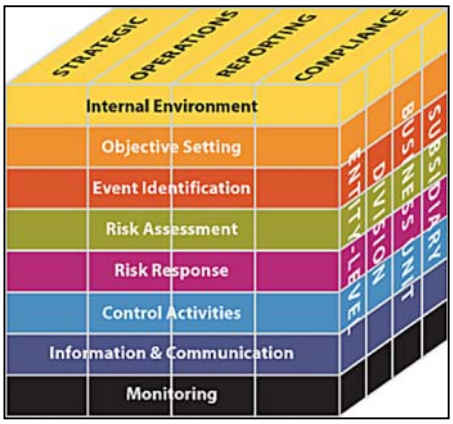

Abbildung 1: Enterprise Risk Management im COSO ERM (2004) Framework. Quelle: (COSO, 2004, p. 5).

Das 2017 novellierte Rahmenwerk "Enterprise Risk Management - Integration with Strategy and Performance" löst sich von dieser Darstellung und verdeutlicht die steigende Bedeutung von Enterprise Risk Management in der strategischen Planung und die ganzheitliche Einbettung in ein Unternehmen. Durch steigende endogene und exogene Anforderungen ist der Umgang mit Risiken ein wesentlicher Bestandteil der Unternehmensstrategie und Unternehmensperformance über alle Abteilungen und Funktionen hinweg. Das neue Rahmenwerk selbst besteht aus 20 Prinzipien, die in fünf miteinander verbundenen Komponenten gegliedert sind und sich folgendermassen zusammensetzen (COSO, 2017, p. 6):

- Governance & Culture: Die Governance bestimmt den "Ton der Organisation" und stärkt die Bedeutung und Verantwortung für die Aufsicht des Risikomanagements. Kultur bezieht sich auf ethische Werte, erwünschte Verhaltensweisen und das unternehmensweite Verständnis von Risiken.
- Strategie & Objective-Setting: Im Rahmen der Komponente erfolgt das Zusammenspiel des Enterprise Risk Managements, Strategie und Zielsetzung im strategischen Planungsprozess. Eine Festlegung des Risikoappetits erfolgt auf Basis der Ausrichtung an der Strategie. Die Transmission der Strategie in die operative Praxis durch operationalisierte Geschäftsziele dient der Grundlage für die Identifizierung, Bewertung und Reaktion auf Risiken.
- Performance: Kernaufgabe der Komponente Performance ist die Identifikation und Bewertung von Risiken, die sich auf die Erreichung der Strategie- und Geschäftsziele auswirken können. Hierzu erfolgt zunächst eine Priorisierung der Risiken nach Eintrittshöhe unter Zugrundelegung des Risikoappetits. Nach Risikomitigation und Messung des überbleibenden Risikos erfolgt die Berichterstattung dieses Prozesses an die wichtigsten Risikointeressengruppen.
- Review & Revision: Durch die rollierende Überprüfung der Leistungsmessung kann die Organisation die Wirksamkeit der einzelnen Elemente der Risikomanagements bewerten und bei Notwendigkeit Verbesserungsbestrebungen einleiten.
- Information, Communication & Reporting: Ein funktionierendes Enterprise Risk Management erfordert einen kontinuierlichen Prozess der Beschaffung und Weitergabe notwendiger Informationen aus internen und externen Quellen, sowohl Top-Down, Botton-Up und horizontal.

Abbildung 2: Enterprise Risk Management im COSO II ERM (2017) Framework. Quelle: (COSO, 2017, p. 6).

3 Risk Governance and Culture

Im Rahmen der Komponente Governance & Culture erfolgt die konstitutive Festlegung der Governance- und Organisationsstruktur des Risikomanagementsystems. Durch die Formulierung von Werten, erwünschten Verhaltensweisen und das unternehmensweite Grundverständnis von Risiken wird weiterhin die Risikokultur des Unternehmens bestimmt. Das COSO schlägt hierzu die Etablierung und Umsetzung der folgenden sechs Prinzipien vor (COSO, 2016, p. 27):

Ausübung der Risikoüberwachungsfunktion des Boards
Im Rahmen der Managementunterstützungsfunktion, zur Erreichung der Strategie- und Geschäftsziele, übernimmt das Board die Aufgabe des Aufsichtsorgans und etabliert Risk Governance-Funktionen in die Organisationsstruktur (COSO, 2016, p. 27). Zur Sicherstellung der Aufsichtsfunktion schlägt das COSO die Etablierung eines Risk Committee und die Erstellung einer Charter zur Dokumentation der Verantwortlichkeiten des Managements und des Aufsichtsgremiums fest. Neben einer ausreichenden Qualifikation und Erfahrung stellt die Unabhängigkeit der Board-Mitglieder einen wesentlichen Erfolgsfaktor für eine objektive Risikoüberwachung dar (COSO, 2016, p. 28f).

Etablierung einer Governance und eines Geschäftsmodells
Ein wesentlicher Erfolgsfaktor eines Risikomanagementsystems stellt die Entwicklung betrieblicher Governance-Strukturen zur Verfolgung von Strategie- und Geschäftszielen dar (COSO, 2016, p. 27). Dies erfolgt insbesondere durch die Bestimmung von festgelegten Berichtslinien anhand der Wertschöpfungskette des Geschäftsmodells. Unter der Berücksichtigung des internen und externen Unternehmensumfeldes muss die kontinuierliche Informationsversorgung des Boards - sei es durch standardisierte Kommunikationswege des operativen Bereiches oder durch Eskalationsmechanismen bei wesentlichen Tatbeständen z.B. überfällige Massnahmen im Follow-Up der Internen Revision - sichergestellt werden (COSO, 2016, p. 30). Eine wesentliche Aufgabe zur Sicherstellung der risikorelevanten Informationsbedürfnisse in der Organisation übernimmt das Risk Committe (COSO, 2016, p. 31). Je nach Komplexität des Geschäftsmodells dient das RM-Committee in der Praxis neben dem Austausch der Bereichs- und Abteilungsleitung mit Risikoverantwortung auch der Einbindung von anderen Governance-Funktionen wie IKS, Compliance und Internal Audit im Sinne des Three-Lines-of-Defense-Modells (The Institute of Internal Auditors, 2013).

Neben der Etablierung eines Committees empfiehlt das COSO die Ernennung eines Chief Risk Officers (CRO) aus den Reihen des Managements zur Koordination und Leitung des unternehmensweiten Risikomanagements (COSO, 2016, p. 31).

Definition des gewünschten Organisationsverhaltens
Die Abhängigkeit des gewünschten Organisationsverhalten erfolgt per Definition der Risikokultur des Unternehmens. Als Stellschraube dient hierzu die Festlegung des Risikoappetits. Auf Grundlage entscheidungstheoretischer Überlegungen erfolgt die Festlegung der Risikoneigung in der Bandbreite Risikoaversion bis zur Risikoaffinität

(COSO, 2016, p. 32 f.). Aus ökonomischer Sicht eignet sich zur fundierten Entscheidungsfindung die Hinzuziehung von mathematischen Verfahren wie z.B. die Sicherheitsäquivalenzmethode oder das Risiko-Chancen-Kalkül aus der Bankbetriebswirtschaftslehre (Schierenbeck, Lister, & Kirmße, 2008, p. 44 ff.).

Bekenntnis zur Integrität und Ethik
Ein unternehmensweites Bekenntnis zur Integrität und ethischen Grundwerten kann durch die Veröffentlichung und Etablierung eines Code of Conducts erreicht werden. Der CoC kodifiziert neben gesetzlichen und ethischen Grundwerten vor allem auch die in der Organisation akzeptierten und nicht akzeptierten Verhaltensweisen. Durch die Durchführung von regelmässigen Trainingsmassnahmen und das Vorleben der Werte durch das Management im Sinne des "Tone at the Top" kann eine steigende Sensibilisierung für die Risikokultur erreicht werden (COSO, 2016, p. 34 f.).

Durchsetzung der Rechenschaftspflicht
Im Rahmen der Governance sind für das Risikomanagement verantwortliche Einzelpersonen auf allen Ebenen der Unternehmung und entsprechende Standards und Leitlinien zur Dokumentation der Verantwortlichkeit festzulegen. Die Gesamtverantwortung über die Angemessenheit und Wirksamkeit des Risikomanagementsystems obliegt durch Delegation des Boards, der Geschäftsleitung in Form des CEO und CRO (COSO, 2016, p. 37 f.). Hierzu gehört insbesondere:

- Die Erstellung und Durchsetzung eines Code of Conducts,
- Etablierung eines geeigneten Informationssystems,
- Sicherstellung der Zielkonformität der Mitarbeiter mit den Geschäftszielen durch geeignete Incentivierungsmassnahmen,
- Etablierung von geeigneten Sanktionsmechanismen für Fehlverhalten und Leistungsevaluationen (COSO, 2016, p. 38).

Rekrutierung, Entwicklung und Erhaltung von Talenten
Zur Erreichung der Strategie und Geschäftsziele benötigt die Gesellschaft den Aufbau eines strategiekonformen Personalmanagements. Hierzu sind zunächst die benötigten Fähigkeiten, Erfahrungen und Kompetenzen der Mitarbeiter zu bestimmen. Die Dokumentation der auf diesem Wege entstehenden Anforderungsprofile erfolgt in Form von Stellenbeschreibungen. Neben der Definition der Soll-Skills müssen entsprechende Massnahmen zur Rekrutierung von neuen Mitarbeitern und die Entwicklung der bestehenden implementiert werden. (COSO, 2016, p. 40 f.).

4 Risk Governance and Culture im Rahmen eines ganzheitlichen ESG-Risk Managements: Erste empirische Erkenntnisse

Die thematische Auseinandersetzung mit Environmental-, Social- und Governance Risiken besitzt aus unternehmerischer Praxis eine steigende Relevanz. Neben der gesetzlichen Verpflichtung zur Offenlegung einer nichtfinanziellen Erklärung in Folge der Umsetzung des europäischen CSR-Richtlinie 2013/34/EU, besteht empirische Evidenz einer positiven Honorierung einer Offenlegung von CSR-Informationen am Kapitalmarkt (Dhaliwal, Li, Tsang, & Yang, 2011; El Ghoul, Guedhami, Kwok, & Mishra, 2011).

Das COSO und das WBCSD folgt diesem Trend und erweitertet das ERM Framework um ESG bezogene Fragestellungen (COSO & WBCSD, 2018). Zur Adressierung des erweiterten Risikoumfangs muss aus Ebene der "Risk Governance and Culture" ein Bewusstsein fürs ESG-Faktoren im Management und in der Ablauforganisation geschaffen werden. Weiterhin sind Berichtswege und Verantwortlichkeiten entsprechend anzupassen und bei Vorliegen von Regelungslücken, Richtlinien und Code of Conduct entsprechend zu ergänzen (COSO & WBCSD, 2018, p. 15 ff.).

Auf Basis einer Querschnittsuntersuchung soll die Risikopublizität im Zuge der nichtfinanziellen Erklärung vor dem Hintergrund des CSR-Richtlinien Umsetzungsgesetzes untersucht werden. Ziel der Untersuchung liegt in der Gewinnung erster empirischer Erkenntnisse zur Interaktion der handelsrechtlichen Lageberichterstattung und des ESG-Risikomanagements regulierter Institutionen. Auf Grundlage der Ergebnisse sollen Best- und Good-Practices der Berichtspraxis identifiziert und Handlungsempfehlungen für den Berichtsersteller und Regulator aufgezeigt werden. Insbesondere soll der Fokus der Untersuchung auf Angaben zur Risk Governance und Unternehmenskultur liegen.

5 Zusammenfassung

Das neue COSO ERM Framework ermöglicht eine verbesserte Anbindung des Risk Managements an den unternehmensweiten Prozess der Strategieentwicklung. Durch den Leitgedanken eines integrierten Governance-Systems ermöglicht das Framework bei vollständiger Adaption eine verbesserte Unterstützung im Strategietransmissionsprozess des Unternehmens.

Die Komponente Risk Governance & Culture liefert den Anwendern ein konstitutives Rahmenwerk für den Aufbau der Governance zur Etablierung eines ganzheitlichen Risikomanagementansatzes in der Organisation. Weitere Forschungsfelder ergeben sich ergänzend in der Adaption von ESG-Risken im unternehmensweiten Risikomanagementsystem und dessen Offenlegung.

Literaturverzeichnis

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, *24*(6), 521–531.

COSO. (2004). Enterprise Risk Management — Integrated Framework (Executive Summary). *New York*, *3*(September), 1–16.

COSO. (2016). *Enterprise Risk Management Aligning Risk with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission.

COSO. (2017). *Enterprise Risk Management Integrating with Strategy and Performance (Executive Summary)*. *Committee of Sponsoring Organizations of the Treadway Commission*. Retrieved from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

COSO, & WBCSD. (2018). *Applying enterprise risk management to environmental, social and governance-related risks. Preliminary Draft*.

Dhaliwal, D. S., Li, O. Z., Tsang, A., & Yang, Y. G. (2011). Voluntary nonfinancial disclosure and the cost of equity capital: The initiation of corporate social responsibility reporting. *Accounting Review*, *86*(1), 59–100.

El Ghoul, S., Guedhami, O., Kwok, C. C. Y., & Mishra, D. R. (2011). Does corporate social responsibility affect the cost of capital? *Journal of Banking and Finance*, *35*(9), 2388–2406.

Hunziker, S., & Balmer, P. (2018). Enterprise Risk Management in Schweizer Unternehmen - Empirische Ergebnisse basierend auf dem neusten COSO ERM Rahmenwerk Entwurf 2016. In S. Hunziker & J. O. Meissner (Eds.), Ganzheitliches Chancen- und Risikomanagement- Interdisziplinäre und praxisnahe Konzepte (pp. 89–111). Wiesbaden.

Hunziker, S., Balmer, P., & Schellenberg, C. (2016). Enterprise Risk Management 2016 - Studie zum Risikomanagement in Schweizer Unternehmen. Zug.

Schierenbeck, H., Lister, M., & Kirmße, S. (2008). *Ertragsorientiertes Bankmanagement, Band 2: Risiko-Controlling und integrierte Rendite-/Risikosteuerung* (9., aktual).

The Institute of Internal Auditors. (2013). *IIA Position Paper : THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL*. Retrieved from https://na.theiia.org/standards-guidance/Public Documents/PP The Three Lines of Defense in Effective Risk Management and Control.pdf

WBCSD. (2017). *Sustainability and enterprise risk management: The first step towards integration*. *Wbcsd*. Retrieved from www.wbcsd.org