Aktuelle Entwicklungen in Governance, Risikomanagement und Interner Steuerung und Kontrolle

Eine Standortbestimmung für das Interne Audit



T. Flemming Ruud ist Professor für Betriebswirtschaftslehre, insbesondere Internal Control/Internal Audit, an der Universität St. Gallen. Zusätzlich ist er ständiger Gastprofessor für Internes und Externes Audit an der Norwegian Business School, Oslo, Norwegen. Viele Jahre war er Vorstandsmitglied des Schweizerischen Verbands für Interne Revision (SVIR). Er berät verschiedene europäische Verbände, Wirtschaftsprüfungsunternehmen, Regierungen und Unternehmen in den Bereichen Corporate Governance, finanzielles und operationelles Auditing. Seine Forschungsschwerpunkte umfassen Internal Control, Internes und Externes Audit, finanzielle Aspekte der Corporate Governance und das Risikomanagement.



Katharina Schramm ist Doktorandin am Lehrstuhl für Internal Control/Internal Audit an der Universität St. Gallen. Zuvor studierte sie im Bachelor Betriebswirtschaftslehre an der Universität Mannheim sowie im Master Accounting & Finance und International Management (CEMS) in St. Gallen und in Barcelona. Sie ist seit 2010 ausgebildete Bankerin. Ihre Forschungsinteressen umfassen Internal Audit, Corporate Governance, interne Kommunikation und Wirtschaftsethik.

Inhaltsverzeichnis

1. Einleitung ... 205

2. Studie zur Internen Steuerung und Kontrolle ... 208
2.1 Beschreibung der Studie und der Studienergebnisse ... 208
2.2 Implikationen für das Interne Audit ... 214

3. Update des COSO ERM Frameworks ... 215
3.1 Beschreibung der Neuerungen ... 215
3.2 Implikationen für das Interne Audit ... 220

4. Möglichkeiten und Grenzen des Three-Lines-of-Defense-Modells ... 221
4.1 Beschreibung des Sachverhalts ... 221
4.2 Implikationen für das Interne Audit ... 225

5. Einordnung und Ausblick ... 225

Literaturverzeichnis ... 228

1. Einleitung

Vorangetrieben durch das Element des Wertbeitrags des Internen Audits *(«to add value»)* haben sich in den vergangenen zwei Dekaden sowohl Wissenschaftler als auch Praktiker die Frage gestellt: *«Wie kann das Interne Audit einen Wertbeitrag für seine internen Anspruchsgruppen und für das Unternehmen als solches erbringen?»* Folgt man der Definition des Internen Audits und der Definition des Wertbeitrags des IIA, so kann geschlussfolgert werden, dass die drei Kernarbeitsgebiete Governance, Risikomanagement und Interne Steuerung und Kontrolle trotz der hohen Dynamik im Berufsstand weiterhin ein grosses Potenzial für wertschaffende Tätigkeiten bieten. Aus diesem Grund stehen diese drei Gebiete im Fokus des vorliegenden Beitrags, dessen theoretischer und struktureller Rahmen nachfolgend kurz vorgestellt und begründet werden soll.

Gemäss Standard 2100 *Art der Arbeiten* des International Professional Practices Framework [IPPF] des Institute of Internal Auditors [IIA][1] soll das Interne Audit die Governance-, Risikomanagement- und Kontrollprozesse der Organisation bewerten sowie zu deren Verbesserung beitragen. Die drei Standards 2110 *Governance,* 2120.A1 zum Risikomanagement sowie 2130.A1 zur Internen Steuerung und Kontrolle [IKS] konkretisieren und ergänzen Standard 2100 inhaltlich. Standard 2110 besagt, dass das Interne Audit zur Verbesserung der Governance-Prozesse der Organisation die strategischen und operativen Entscheidungen, die Beaufsichtigung von Risikomanagement und -steuerung, die Förderung ethisch angemessener Normen und Werte in der Organisation, die Sicherstellung einer wirksamen Leistungssteuerung und -messung sowie klarer Verantwortlichkeiten, die Kommunikation von Risiko- und Kontrollinformationen an die zuständigen Funktionen sowie die Koordination der Aktivitäten von und Kommunikation zwischen Geschäftsleitung und Verwaltungsrat, externen und internen Prüfern, anderen Prüfungsdienstleistern sowie operativem Management beurteilen und diesbezüglich angemessene Empfehlungen geben soll. Standards 2120.A1 und 2130.A1 sehen vor, dass das Interne Audit die Risikopotenziale in Governance, in den Geschäftsprozessen und Informationssystemen bzw. zusätzlich die Angemessenheit und Wirksamkeit der Kontrollen bewerten bzw. beurteilen soll in Bezug auf die Erreichung der strategischen Ziele der Organisa-

1 Vgl. The Institute of Internal Auditors (2017).

tion, die Zuverlässigkeit und Integrität von Daten des Rechnungswesens und von operativen Informationen, die Effektivität und Effizienz von Geschäftsprozessen und Programmen, die Sicherstellung des Betriebsvermögens und die Einhaltung von Gesetzen, Verordnungen, Richtlinien, Verfahren und Verträgen.

Wie aus den vorgängig erläuterten Standards ersichtlich wird, übernimmt das Interne Audit innerhalb der Arbeitsgebiete Governance, Risikomanagement und Interne Steuerung und Kontrolle diverse Tätigkeiten, die darauf ausgerichtet sind, die Geschäftsprozesse zu verbessern und zur Zielerreichung des Unternehmens beizutragen. Vor allem zwischen den Gebieten Risikomanagement und Interner Steuerung und Kontrolle sind inhaltliche Überschneidungen vorzufinden. Dies entspricht auch dem Verständnis des *Committee of the Sponsoring Organizations of the Treadway Commission* [COSO],[2] nach dem die Interne Steuerung und Kontrolle einen Teilbereich des Risikomanagements darstellt, welches wiederum ein Element der Governance als Ganzes ist. Folglich könnte das Interne Audit auch als zentrales Instrument des Verwaltungsrats für eine wirksame Governance interpretiert werden.

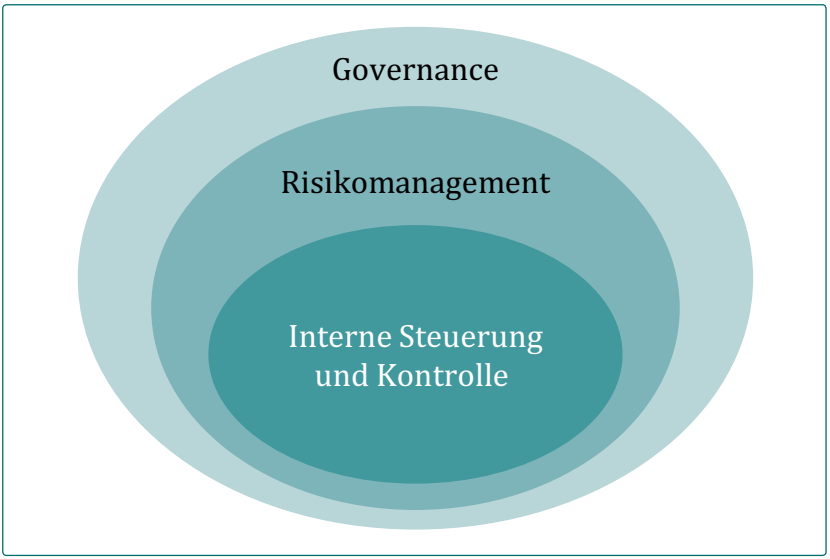


Abb. 1: Zusammenhang zwischen Governance, Risikomanagement und Interner Steuerung und Kontrolle

2 Vgl. Committee of the Sponsoring Organizations of the Treadway Commission (2004, 2013).

Vor diesem Hintergrund gilt es, wichtige Entwicklungen in *Governance, Risikomanagement* und *Interner Steuerung und Kontrolle* zu erörtern sowie mögliche Einflüsse für das Interne Audit abzuwägen. Im Rahmen dieses Beitrags sollen daher drei relevante Aspekte für jedes Arbeitsgebiet aufgezeigt und deren Implikationen für das Interne Audit diskutiert werden. Diese sind im Einzelnen:

1. für das Gebiet *Interne Steuerung und Kontrolle:* die vom Institut für Accounting, Controlling & Auditing der Universität St. Gallen (ACA-HSG) durchgeführte Studie zum aktuellen Stand des Internen Kontrollsystems in Schweizer Nichtfinanzunternehmen[3]
2. für das Gebiet *Risikomanagement:* das 2017 veröffentlichte Update zum COSO Enterprise Risk Management [COSO ERM] Framework[4]
3. für das Gebiet *Governance:* Möglichkeiten und Grenzen des Three-Lines-of-Defense-Modells[5]

Das übergeordnete Ziel ist es, dem Leser einen Überblick über die wichtigsten Entwicklungen im Berufsstand zu vermitteln und auch fachfremde Personen mit den Arbeiten des Internen Audits besser vertraut zu machen. Dabei soll primär auf die drei Arbeitsgebiete abgestellt und weniger auf Details – zum Beispiel im Hinblick auf den Audit-Prozess – eingegangen werden.

Den obigen Überlegungen folgend ist der Beitrag in vier grössere Teile aufgegliedert. Nach der thematischen und strukturgebenden Einführung in *Kapitel 1* folgt die Erörterung der Entwicklungen aus den Bereichen Interne Steuerung und Kontrolle in *Kapitel 2*, Risikomanagement in *Kapitel 3* und Governance in *Kapitel 4*. In jedem dieser Kapitel sollen auch mögliche Auswirkungen für die Arbeiten des Internen Audits diskutiert werden. Abschliessend wird der Beitrag in *Kapitel 5* in einen grösseren Gesamtzusammenhang eingeordnet, bei dem unter anderem auch weitere zukunftsweisende Tendenzen rund um das Interne Audit kurz vorgestellt werden.

3 Vgl. Ruud, Kyburz und Schramm (2018).

4 Vgl. Committee of the Sponsoring Organizations of the Treadway Commission (2017).

5 Vgl. European Confederation of Institutes of Internal Auditing/Federation of European Risk Management Associations (2010).

2. Studie zur Internen Steuerung und Kontrolle

2.1 Beschreibung der Studie und der Studienergebnisse

Der Nachweis der *Existenz* eines IKS ist für Unternehmen, die nach Art. 727 Abs. 1 OR zu einer ordentlichen Revision verpflichtet sind, obligatorisch. Zudem können die Erwartungen der externen Anspruchsgruppen an eine wirksame Governance dazu führen, dass auch nicht ordentlich geprüfte Unternehmen die bei Wettbewerbern etablierten Kontrollstrukturen zum Zweck eines positiven Signals übernehmen. Neben der reinen Existenz interessiert vor allem, wie wirksam und nachhaltig das IKS in Schweizer Unternehmen eingerichtet ist. Vor diesem Hintergrund wurde im Jahr 2018 am ACA-HSG eine Studie zum aktuellen Stand des IKS in Schweizer Unternehmen ausserhalb des Finanzsektors abgeschlossen. An dieser Studie nahmen insgesamt 64 Unternehmen teil, deren Repräsentanten mehrheitlich Finanzleiter (64%) und Leiter des IKS (42%) waren. Neben der Verbreitung von einschlägigen Rahmenwerken und der Etablierung von Risiko- und Kontrollfunktionen wurde der Reifegrad des IKS gemäss den einzelnen Komponenten des COSO Internal Control Frameworks (2013) eruiert.

Um Aufschluss über mögliche Unterschiede zwischen verschieden grossen Unternehmen zu gewinnen, wurden die Ergebnisse anhand von drei Grössenkategorien analysiert. Die Unterscheidung zwischen Unternehmensgrössen ist auch deshalb sinnvoll, da tendenziell mit zunehmender Unternehmensgrösse ein höherer Formalisierungsgrad der Internen Steuerung und Kontrolle einhergeht. Die jeweiligen Grössenkategorien sind im Einzelnen:

- kleine Unternehmen mit bis zu 250 Mitarbeitenden
- mittelgrosse Unternehmen mit 250 bis 999 Mitarbeitenden
- grosse Unternehmen ab 1000 Mitarbeitenden

Die zentralen Erkenntnisse der Studie sollen in diesem Kapitel vorgestellt und diskutiert werden. Da bei den Fragen oftmals Mehrfachnennungen möglich waren, können die kumulierten Prozentzahlen nachfolgend mehr als 100% ergeben.

Wie zu erwarten, bestätigen die Studienergebnisse, dass die beiden Rahmenwerke von COSO aus den Jahren 1992 und 2013 im Durchschnitt die bekanntesten Frameworks zur Internen Steuerung und Kontrolle sind, gefolgt von der Norm 31000:2009[6] der International Organization for Standardization [ISO] und dem Modell Control Objectives for Information and Related Technology (2012) [COBIT 5] der Information Systems Audit and Control Association. Betrachtet man die Verbreitung der Rahmenwerke aufgegliedert nach der Unternehmensgrösse, ist jedoch festzustellen, dass bei den kleineren Unternehmen sogar die ISO-Norm bekannter ist als die beiden COSO Frameworks. Für grosse Unternehmen mit einer tendenziell ausgereifteren IT-Infrastruktur ist zudem das COBIT 5 von besonders grosser Bedeutung.

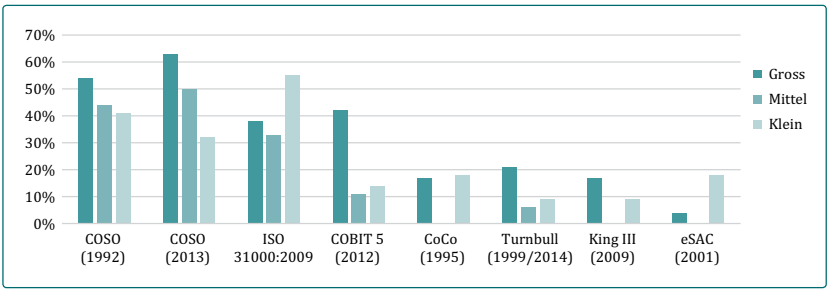


Abb. 2: Bekanntheit von Rahmenwerken nach Unternehmensgrösse

Über alle Unternehmensgrössen hinweg sind die üblichen Kontrollfunktionen (Health, Safety & Environment [HSE], Controlling, Qualitätssicherung, Betriebsschutz, Risikomanagement, Compliance, IKS-Koordinationsstelle) entweder als eigenständige Funktion oder zumindest als Teilfunktion vorhanden. Das Interne Audit ist bei 31% der teilnehmenden Unternehmen eine eigenständige Funktion und bei 22% eine Teilfunktion. Dies hängt womöglich auch damit zusammen, dass das Interne Audit anders im Finanzsektor bei den befragten Unternehmen nicht regulatorisch vorgeschrieben ist.

6 Ein Update zur Norm wurde nach der Durchführung der Studie im Jahr 2018 veröffentlicht.

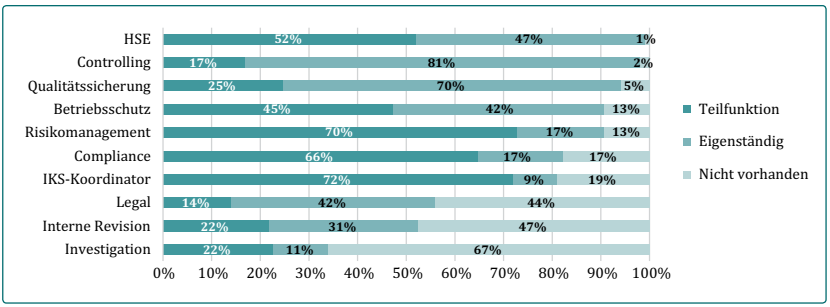


Abb. 3: Risiko- und Kontrollfunktionen in Schweizer Nichtfinanzunternehmen

Mit Blick auf die Gestaltung des IKS wird die IKS-Koordinationsstelle als besonders bedeutsam eingeschätzt, gefolgt vom Controlling und vom Internen Audit. Die Relevanz der einzelnen Aktivitäten für die IKS-Gestaltung hängt dabei auch von der Geschäftsausrichtung und Branchenzugehörigkeit des jeweiligen Unternehmens ab. Aus diesem Grund sehen auch 45% eine zentrale Rolle bei der Qualitätssicherung, 46% bei der Compliance-Abteilung und knapp ein Drittel bei der HSE-Funktion.

Es zeigt sich ausserdem, dass in den teilnehmenden Unternehmen mit dem IKS vor allem Compliance-Ziele sowie Ziele der Finanzberichterstattung verfolgt werden. Weniger häufig werden dagegen Ziele der operativen Geschäftstätigkeit und der Nichtfinanzberichterstattung priorisiert.

Neben den vorgenannten Aspekten ist auch der Reifegrad des IKS und seiner einzelnen Komponenten von Interesse, welcher durch das Reifegradmodell der Carnegie Mellon University ausgewertet wurde.[7] Das Reifegradmodell ist in fünf Maturitätsstufen unterteilt, wobei *anfänglich* die geringste und *optimiert* die höchste Maturität darstellt. Während das IKS bei der anfänglichen Stufe noch ad hoc gestaltet und nicht standardisiert ist, ist die *strukturierte* Stufe bereits durch bestimmte festgelegte Strukturen und Mindestdokumentationen gekennzeichnet. Stufe drei, *etabliert,* beschreibt ein standardisiertes IKS, welches unternehmenseinheitlich angewendet wird. Schliesslich charakterisieren Stufe vier, *geführt,* und Stufe fünf, *optimiert,* ein IKS, welches die Anforderungen der verschiedenen Anspruchsgruppen erfüllt und einen Mehrwert für diese darstellt respektive kontinuierlich weiterentwickelt und verbessert wird.

7 Vgl. Chrissis, Konrad und Shrum (2009).

Die nachfolgenden Abschnitte stellen den von den Befragten wahrgenommenen Reifegrad der fünf Komponenten des bekanntesten Frameworks in der Schweiz, des COSO Internal Control – Integrated Frameworks (2013), welche das Steuerungs- und Kontrollumfeld, die Risikobeurteilung, Steuerungs- und Kontrollaktivitäten, Information und Kommunikation sowie das Monitoring umfassen, vor.

Das *Steuerungs- und Kontrollumfeld* bezieht sich auf die Normen und Werte im Unternehmen, auf die Philosophie und die Arbeitsweise des Verwaltungsrats und der Geschäftsleitung, auf die Regelung von Kompetenzen und Verantwortlichkeiten sowie auf das Personalwesen. Diese Komponente wird hauptsächlich durch die regelmässige Information des Verwaltungsrats über die Interne Steuerung und Kontrolle sowie durch die regelmässige Identifikation von Verbesserungspotenzialen im Bereich des IKS umgesetzt. Darüber hinaus wird das IKS bei 42% der Unternehmen durch ethisch eingestellte Mitarbeiter gelebt und gefördert. Weniger häufig, nur bei 22% respektive bei 20%, beziehen sich Stellenbeschreibungen speziell auf das IKS, oder es werden Verstösse gegen das IKS mit Disziplinarmassnahmen bestraft.

Der Reifegrad des *Steuerungs- und Kontrollumfelds* wird von den teilnehmenden Unternehmen überwiegend als *etabliert* oder als *geführt* eingestuft, wobei kleine Unternehmen diesen tendenziell etwas höher bewerten als mittelgrosse oder grosse Unternehmen. Dies ist gegebenenfalls darauf zurückzuführen, dass Verwaltungsrat und Geschäftsleitung in kleineren Firmen mit flacheren Hierarchien einen unmittelbareren Einfluss auf das Steuerungs- und Kontrollumfeld über den *Tone at the Top* ausüben können. Je stärker die Strukturierung der Prozesse und damit der Grad der Bürokratisierung, desto geringer ist in der Tendenz auch der direkte Einfluss der oberen Governance-Organe auf die Unternehmenskultur.

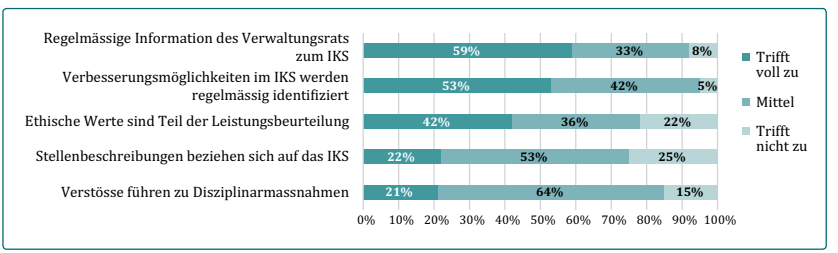


Abb. 4: Ausgestaltung des Steuerungs- und Kontrollumfelds

Die *Risikobeurteilung* wird bei der Mehrheit der Antwortenden einmal jährlich durchgeführt (55%), wobei auch eine halbjährliche (17%), quartalsweise (17%), kontinuierliche (17%) oder eine Risikobeurteilung auf Ad-hoc-Basis (22%) angewendet werden. Verschiedene Aspekte werden in der Risikobeurteilung herangezogen und berücksichtigt, welche in der nachfolgenden Abbildung genauer dargestellt sind. Besonders zu bemerken ist, dass 30% auch Chancen beurteilen. Insgesamt wird der Reifegrad der zweiten Komponente leicht höher eingeschätzt als der des *Steuerungs- und Kontrollumfelds*. So bewertet mindestens die Hälfte der Befragten ihre Risikobeurteilung durchschnittlich entweder als *optimiert* oder als *geführt*.

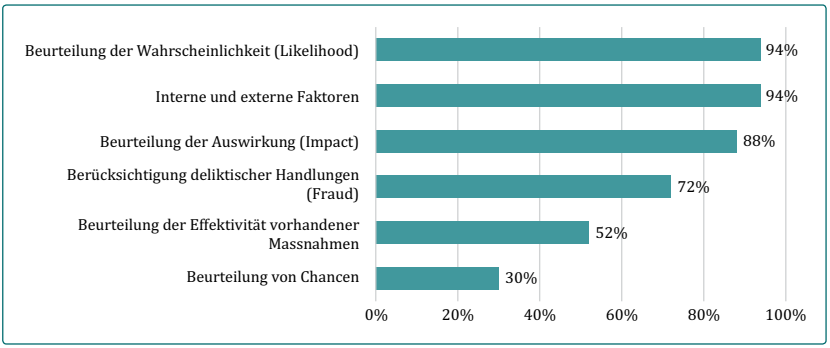


Abb. 5: Ausgestaltung der Risikobeurteilung

Die *Steuerungs- und Kontrollaktivitäten* stellen die dritte Komponente des IKS gemäss COSO (2013) dar. Durch sie werden die vorgängig identifizierten Risiken nach Massgabe des vom Verwaltungsrat bestimmten Risikoappetits gehandhabt. Die Studienergebnisse verdeutlichen, dass vor allem die *direktiven* (steuernden) Massnahmen wie zum Beispiel Richtlinien oder Prozessbeschriebe am häufigsten angewendet werden, gefolgt von *präventiven* (vorbeugenden), *korrektiven* (korrigierenden) und schliesslich *detektiven* (aufdeckenden) Massnahmen. Damit wählen die Unternehmen im Durchschnitt einen relativ ökonomischen Ansatz, bei dem negative Ereignisse bestenfalls bereits vor ihrem Eintritt antizipiert und vermieden werden. Konkret kommen am häufigsten das Vieraugenprinzip (97%), Genehmigungsverfahren (95%), Budgetvergleiche und Analysen (94%), die Funktionentrennung (92%) oder Kontenabstimmungen (86%) zum Einsatz. Grosse Unternehmen schätzen den Reifegrad dieser Komponente insgesamt am höchsten ein. 65% der Teilnehmer die-

ser Grössenkategorie beurteilen die Maturität entweder als *optimiert* oder als *geführt*. Bei mittleren Unternehmen entspricht dies der Wahrnehmung von 40%, bei kleineren Unternehmen immerhin von der Hälfte.

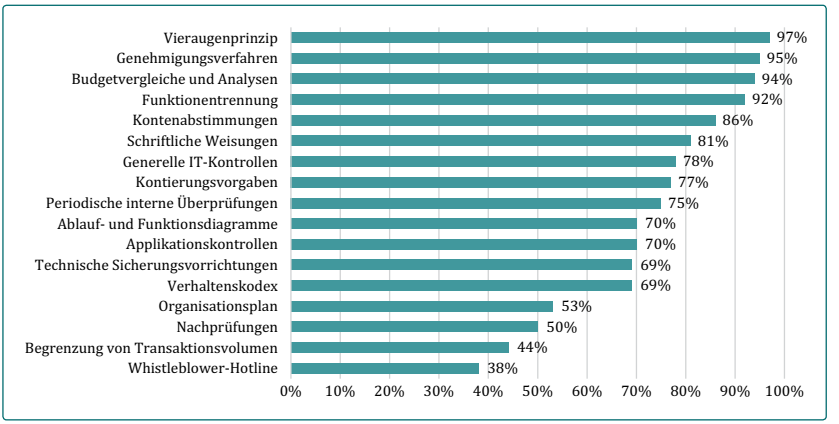


Abb. 6: Ausgestaltung der Steuerungs- und Kontrollaktivitäten

Damit das IKS wirksam ist, müssen die zentralen Aspekte der Internen Steuerung und Kontrolle über alle Unternehmensebenen hinweg kommuniziert werden. Am häufigsten geschehen die *Information* und *Kommunikation* bezüglich des IKS über Regelungen und Weisungen (84%), Ad-hoc-Mitteilungen (55%), Veranstaltungen auf Abteilungsebene (39%), Präsenzschulungen (38%), Veranstaltungen auf Unternehmensebene (25%) oder E-Learning (25%). Grosse Unternehmen betrachten die Information und Kommunikation zum IKS zu 47% als *geführt*, bei kleinen und mittleren Unternehmen sind dies 18% respektive 16%.

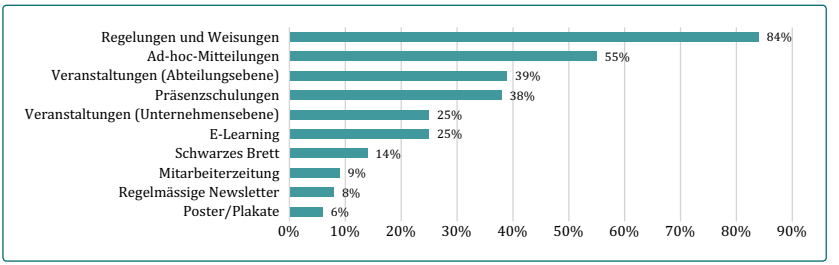


Abb. 7: Ausgestaltung der Information und Kommunikation

Beim *Monitoring* kann zwischen separaten Beurteilungen und laufendem Monitoring differenziert werden. Separate Beurteilungen, die meist an

einen bestimmten Auslöser wie ein spezielles Ereignis oder einen Zeitpunkt geknüpft sind, kommen vor allem bei grossen (59%) und kleinen Unternehmen (55%) besonders stark zum Tragen, während mittelgrosse Unternehmen hauptsächlich Ad-hoc-Prüfungen durchführen (48%). Überraschend ist, dass knapp ein Viertel der grossen Unternehmen sowie ein Fünftel der mittelgrossen Unternehmen angeben, noch kein systematisches IKS-Monitoring eingerichtet zu haben. Die Maturität des *Monitorings* wird von kleinen Unternehmen mit Blick auf die oberen zwei Reifegradstufen höher eingestuft als von mittelgrossen und grossen Unternehmen.

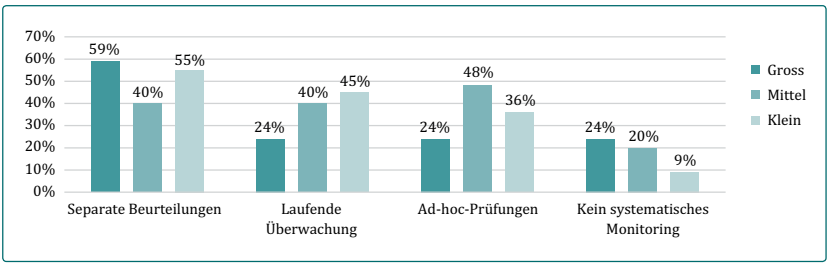


Abb. 8: Ausgestaltung des Monitorings

Im Anschluss an die Eruierung der einzelnen Reifegrade wurden von den Teilnehmenden mögliche Verbesserungspotenziale für die künftige Ausgestaltung identifiziert. Die Ergebnisse zeigen dabei ein klares Bild. So gibt mehr als die Hälfte (56%) an, dass das IKS durch eine bessere Verankerung im Bewusstsein der Mitarbeitenden gefördert werden kann. Zusätzlich identifizieren die teilnehmenden Unternehmen grosses Potenzial in der Anpassung des IKS an Veränderungen (45%), im Monitoring und in der kontinuierlichen Verbesserung (38%), in der Zuweisung personeller Ressourcen (30%) oder in der Beurteilung der Unternehmensrisiken (25%). Während das Monitoring und die Verbesserung des IKS vor allem von grossen Unternehmen genannt werden, priorisieren kleine Unternehmen besonders stark das verfügbare Budget.

2.2 Implikationen für das Interne Audit

Die Aufgaben des Internen Audits im Rahmen der Internen Steuerung und Kontrolle sind über IIA Standard 2130 geregelt. Über diese Ausführungen hinaus kann das Interne Audit vor allem über die Verankerung des IKS in der Unternehmenskultur, über die Empfehlung von IKS-Anpas-

sungen in Prüfberichten, über ein verbessertes IKS-Monitoring sowie über die Information und Kommunikation von IKS-relevanten Aspekten zur künftigen Optimierung beitragen.

Konkret kann es wichtige Sachverhalte an den Verwaltungsrat und an die Geschäftsleitung rapportieren und empfehlen, zum Beispiel über den *Tone at the Top* mehr Bewusstsein zu schaffen, bestimmte Veränderungen bei den Komponenten einzuleiten, oder neue Verantwortlichkeiten für das Monitoring festlegen. Das Interne Audit stellt ein wichtiges Verbindungsglied zwischen den operativen Einheiten und den strategischen Entscheidungsträgern dar und trägt zu einem harmonisierten Verständnis der Internen Steuerung und Kontrolle über alle Unternehmensebenen hinweg bei.

3. Update des COSO ERM Frameworks

3.1 Beschreibung der Neuerungen

Im Jahr 2017 erschien eine überarbeitete Fassung des COSO Enterprise Risk Management Frameworks unter dem Titel «Enterprise Risk Management – Integrating with Strategy and Performance». Ausgangslage für die Revision waren die global steigende Volatilität, Komplexität und Ambiguität der Risiken, die sich auch auf Unternehmensebene auswirken können. Eine der zentralen Anpassungen im neuen COSO ERM Framework ist der stärkere Bezug zwischen der Unternehmensstrategie und der Handhabung der Risiken. Zum einen soll das Risikomanagement angemessen sicherstellen, dass die Strategie in Einklang mit der Mission und den zentralen Werten des Unternehmens steht. Zum anderen steigert ein effektives Risikomanagement die Wahrscheinlichkeit, dass Verwaltungsrat und Geschäftsleitung den richtigen Strategieentscheid treffen, da alle wesentlichen Risiken und Chancen berücksichtigt und beurteilt wurden. Vor diesem Hintergrund gilt ein unternehmensweites Risikomanagement als wirksam, wenn

- die gesamte Bandbreite der Möglichkeiten, dies bedeutet sowohl Risiken als auch Chancen, beachtet und ausgeschöpft wird;
- Risiken über alle Unternehmensebenen hinweg identifiziert und gehandhabt werden, damit Risikoursprung und Risikofolge in einen Sachzusammenhang gebracht werden können;

- die Wahrscheinlichkeit negativer Überraschungen durch zuvor unberücksichtigte Risiken und damit verbundene Kosten und Verluste reduziert sowie der Eintritt günstiger Entwicklungen gefördert werden;
- die Variabilität des Unternehmenserfolgs als Folge des unternehmensweiten Risikomanagements geschmälert wird;
- die Zuteilung und der Verbrauch von Unternehmensressourcen möglichst ökonomisch erfolgen;
- die Resilienz des Unternehmens durch die verbesserte Fähigkeit, Risiken zu antizipieren, auf Veränderungen zu reagieren sowie sich weiterzuentwickeln und langfristig erfolgreich zu sein, gesteigert wird.[8]

Den obigen sechs Leitaspekten für ein effektives unternehmensweites Risikomanagement liegt die Gemeinsamkeit zugrunde, dass die Steigerung des nachhaltigen Unternehmenserfolgs übergeordnetes Ziel sein soll. Dieser wird durch eine Vielzahl von Faktoren bestimmt, welche die Unternehmensziele und die Unternehmenskultur einschliessen. Daher bezeichnet Enterprise Risk Management erweitert nun auch «*die Kultur, Fähigkeiten und Methoden, integriert mit der Strategiefestlegung und dem Unternehmenserfolg, auf die sich Unternehmen abstützen, um Risiken bei der Schaffung, Erhaltung und Verwirklichung von Mehrwert zu handhaben*».[9]

Bestimmte Aspekte dieser Definition treten besonders in den Fokus, auf die nachfolgend in der Reihenfolge ihrer Erwähnung kurz erläuternd eingegangen werden soll.

- *Unternehmenskultur:* Die Unternehmenskultur wird geprägt von den Einstellungen und Handlungen der Mitarbeitenden und beeinflusst diese wiederum im Umkehrschluss. Das unternehmensweite Risikomanagement muss daher in einem engen Zusammenhang mit der Unternehmenskultur stehen.
- *Fähigkeiten:* Das unternehmensweite Risikomanagement unterstützt dabei, die Fähigkeiten aufzubauen, die für die Ausübung der Mission und der Vision des Unternehmens benötigt werden und die dabei helfen, Herausforderungen frühzeitig zu antizipieren.

8 Vgl. The Committee of the Sponsoring Organizations of the Treadway Commission (2017), S. 6 f.

9 Vgl. The Committee of the Sponsoring Organizations of the Treadway Commission (2017), S. 10.

- *Methoden:* Methoden dienen zum besseren Verständnis der Unternehmensstrategie, der Geschäftsziele, der korrespondierenden Risiken, des akzeptierten Risikoniveaus, des Einflusses der Risiken auf den Unternehmenserfolg und der Möglichkeiten zur Handhabung der Risiken.
- *Integration mit Strategiefestlegung und Unternehmenserfolg:* Das unternehmensweite Risikomanagement ist untrennbar verknüpft mit der Festlegung der Strategie, mit dem Verständnis des Risikoprofils und den Implikationen alternativer Strategien auf dieses Risikoprofil.
- *Risikohandhabung:* Es soll sichergestellt werden, dass der Verwaltungsrat und die Geschäftsleitung eine angemessene Erwartung haben, dass das akzeptierte Risikoniveau für die Erreichung der Unternehmensstrategie und der Geschäftsziele angemessen ist.
- *Mehrwert:* Das unternehmensweite Risikomanagement unterstützt dabei, eine Strategie zu wählen, die den erwarteten nachhaltigen Mehrwert mit dem Risikoappetit des Unternehmens sowie den benötigten Fähigkeiten in Verbindung bringt.[10]

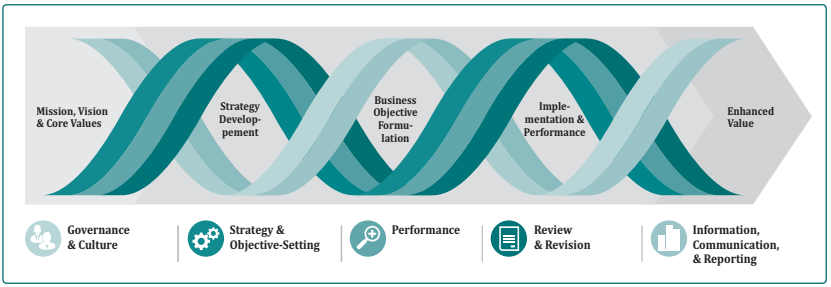


Abb. 9: Grafische Darstellung des neuen COSO ERM

Analog zum ursprünglichen COSO ERM Framework (2004) ist das unternehmensweite Risikomanagement auch in der Neufassung in Komponenten mit zugeordneten Prinzipien untergliedert, diese sind jedoch stärker auf die Aspekte Kultur, Strategie und Unternehmenserfolg ausgerichtet. Die früher acht Komponenten – *Kontrollumfeld, Zielsetzung, Risikoidentifikation, Risikobeurteilung, Risikosteuerung, Kontrollmassnahmen, Information und Kommunikation* sowie *Monitoring* – wurden um drei Komponenten verkürzt. Obwohl sich alle ursprünglichen Komponenten inhaltlich in den neuen Komponenten widerspiegeln, ist

10 Vgl. The Committee of the Sponsoring Organizations of the Treadway Commission (2017), S. 10 ff.

die Trennung im Vergleich weniger klar und schwieriger zu durchblicken. So werden die früher getrennten Komponenten *Risikoidentifikation, Risikobeurteilung* und *Risikosteuerung* nun in einer einzelnen Komponente – *Unternehmenserfolg* – gebündelt.

Die insgesamt 20 Prinzipien für alle fünf Komponenten umfassen jeweils zwischen zwei und sechs Wörter und sind bewusst prägnant formuliert. Zu jedem Prinzip werden Beispiele entweder im Text oder auch als Grafik bzw. in Tabellenform gegeben. Aus dem hohen Abstraktionsgrad der Prinzipien kann abgeleitet werden, dass diese zwar als Anhaltspunkt betrachtet werden können, den Unternehmen aber gleichzeitig noch genügend Flexibilität bei der individuellen Umsetzung zugestanden wird. Übersetzt aus dem Englischen werden die einzelnen Komponenten mit den korrespondierenden Prinzipien wie folgt dargestellt.

Governance und Kultur (Governance & Culture)	• übt Aufsicht über Risiken in Verwaltungsrat und Geschäftsleitung aus *(Exercises Board Risk Oversight)* • etabliert operative Strukturen *(Establishes Operating Structures)* • definiert die Zielkultur *(Defines Desired Culture)* • beweist Verpflichtung zu zentralen Werten *(Demonstrates Commitment to Core Values)* • zieht fähige Personen an, entwickelt und erhält sie *(Attracts, Develops and Retains Capable Individuals)*
Strategie und Zielsetzung (Strategy & Objective Setting)	• analysiert den Geschäftskontext *(Analyzes Business Context)* • definiert den Risikoappetit *(Defines Risk Appetite)* • beurteilt alternative Strategien *(Evaluates Alternative Strategies)* • formuliert Geschäftsziele *(Formulates Business Objectives)*
Unternehmenserfolg (Performance)	• identifiziert Risiken *(Identifies Risk)* • beurteilt die Schwere der Risiken *(Assesses Severity of Risk)* • priorisiert Risiken *(Prioritizes Risks)* • implementiert Massnahmen zur Risikosteuerung *(Implements Risk Responses)* • entwickelt eine Portfolio-Perspektive *(Develops Portfolio View)*

Überprüfung und Überarbeitung (Review & Revision)	• beurteilt wesentliche Veränderungen *(Assesses Substantial Change)* • überprüft Risiken und Unternehmenserfolg *(Reviews Risk and Performance)* • strebt Verbesserungen an *(Pursues Improvement in Enterprise Risk Management)*
Information, Kommunikation und Berichterstattung (Information, Communication & Reporting)	• setzt Informationen und Technologien wirksam ein *(Leverages Information and Technology)* • kommuniziert Risikoinformationen *(Communicates Risk Information)* • erstattet Bericht über Risiken, Kultur und Unternehmenserfolg *(Reports on Risk, Culture, and Performance)*

Tab. 1: Übersicht über Komponenten und Prinzipien des neuen COSO ERM (2017)[11]

Insgesamt scheint der Kerngedanke des neuen COSO ERM zeitgemäss, gleichzeitig aus pädagogischer Sicht aber auch weniger greifbar als der seiner Vorgängerversion. Die neue Darstellung und die Zusammenführung der Komponenten führen zudem zu einer Verschiebung des Verständnisses von eher technisch anmutenden Aspekten zu weichen Faktoren wie Strategie, Kultur und Mehrwert. Auch Hunziker beurteilt das neue COSO ERM gemischt. Zwar begrüsst er die Grundidee, das unternehmensweite Risikomanagement als *«integrativen Bestandteil guter Unternehmensführung (noch stärker) zu positionieren»*,[12] und hebt neben der Abkehr von der früheren Würfel-Darstellung die Berücksichtigung psychologischer Aspekte wie den Zusammenhang zwischen Risikobeurteilung und Risikokultur positiv hervor. Gleichzeitig sieht er unter anderem einen möglichen Schwachpunkt in den Handlungsempfehlungen für die Risikobeurteilung, da das Update *«keine konsistente Anleitung für die Praxis liefert, wie die Risikobewertung vor dem Hintergrund der (strategischen) Zielerreichung umgesetzt werden kann»*.[13]

Auch ISO hat im Jahr 2018 eine Revision der Norm 31000 zum Risikomanagement veröffentlicht. Wie das COSO ERM besteht diese vielfach aus Prinzipien und Leitgedanken, enthält aber ergänzend noch ein Framework sowie eine Prozessbeschreibung.[14] In ihrer Gesamtheit zielt

11 Vgl. The Committee of the Sponsoring Organizations of the Treadway Commission (2017), S. 22.

12 Vgl. Hunziker (2018), S. 168.

13 Vgl. Hunziker (2018), S. 167.

14 Vgl. International Organization for Standardization (2018).

die neue ISO-Norm schliesslich noch konkreter als das COSO ERM auf die Integration des Risikomanagements in die Geschäftsprozesse ab. Da das COSO-Update trotz vieler Beispiele noch abstrakter konzipiert ist als sein Vorgänger, bleibt abzuwarten, wie gut es speziell im Vergleich zur ISO-Norm 31000:2018 in der Praxis aufgenommen werden wird.

3.2 Implikationen für das Interne Audit

Gemäss IIA Standard 2120[15] muss das Interne Audit die Wirksamkeit der Risikomanagementprozesse beurteilen und zu deren Verbesserung beitragen. Ein wirksamer Risikomanagementprozess führt dazu, dass die Ziele des Unternehmens mit dessen Mission in Einklang stehen und diese unterstützen sowie wesentliche Risiken erkannt und bewertet, angemessene Risikomassnahmen ergriffen und zentrale risikobezogene Informationen rechtzeitig kommuniziert werden. Der Kerngedanke des neuen COSO ERM ist somit im Grundsatz sehr ähnlich zu den Ausführungen in IIA Standard 2120. Daher könnte das Interne Audit durch das neue COSO ERM in der Erfüllung seiner auf das Risikomanagement bezogenen Aufgaben durchaus unterstützt werden. Wird das neue Rahmenwerk schliesslich in der Praxis anerkannt, müssen insbesondere die Internen Auditoren mit dessen zentralen Inhalten vertraut sein. Allenfalls ist mit einem erhöhten Zeitaufwand bei der Prüfung der Risikomanagementprozesse zu rechnen, da das neue COSO-ERM-Modell komplexer formuliert ist als das ursprüngliche Framework und zudem im Vergleich weniger Schnittmengen zum COSO Internal Control – Integrated Framework (2013) vorhanden sind. Folglich könnten Synergien zwischen Risikomanagement und Interner Steuerung und Kontrolle gegebenenfalls schwieriger zu erzielen sein. Ausserdem ist in Anlehnung an die neuen Schwerpunkte ein erweitertes Tätigkeitsfeld des Internen Audits, zum Beispiel in Bezug auf Strategie- oder Kultur-Audits, denkbar.

15 Vgl. The Institute of Internal Auditors (2017).

4. Möglichkeiten und Grenzen des Three-Lines-of-Defense-Modells

4.1 Beschreibung des Sachverhalts

Das Three-Lines-of-Defense-Modell wurde von der *European Confederation of Institutes of Internal Auditors* [ECIIA] und der *Federation of European Risk Management Associations* [FERMA] entwickelt.[16] Gemäss Ruud und Kyburz wurde es als *«Folge der Veröffentlichung der 8. EU-Richtlinie von 2006, der sogenannten Abschlussprüfer-Richtlinie, einem breiteren Publikum präsentiert»* und sollte dazu dienen, *«die betroffenen Unternehmen bei der Umsetzung der neuen Vorgaben zu unterstützen»*.[17] Der übergeordnete Zweck des Modells ist die lückenlose und ökonomische Regelung der Aufgaben und Verantwortlichkeiten vor dem Hintergrund einer wirksamen Internen Steuerung und Kontrolle, eines funktionierenden Risikomanagements sowie einer guten Corporate Governance als Ganzes. Konkret wird im Modell die Verantwortung primär für Risikobeurteilung, Steuerungs- und Kontrollaktivitäten, Information und Kommunikation und das Monitoring des IKS auf drei sogenannte Verteidigungslinien, die jeweils aus verschiedenen Governance-Funktionen bzw. Aktivitäten bestehen, aufgeteilt.[18] Die erste Linie führt die prozessintegrierten Kontrollen *(Risk Owner)*, die zweite Linie die prozessnahen Kontrollen *(Risk Control)* und die dritte Linie – das Interne Audit – die prozessunabhängigen Kontrollen *(Risk Assurance)* durch. Jede Linie soll das inhärente Risiko somit schrittweise auf das vom Verwaltungsrat akzeptierte Risikoniveau reduzieren.[19] Einzig das Interne Audit hat neben einer administrativen Berichterstattungslinie an die Geschäftsleitung zusätzlich eine direkte Berichterstattungslinie an den Verwaltungsrat und ist somit vom Management funktional unabhängig. Verwaltungsrat und Geschäftsleitung sind verantwortlich für die Etablierung eines angemessenen Steuerungs- und Kontrollumfelds, welches durch das Interne Audit geprüft und verbessert werden kann.

16 European Confederation of Institutes of Internal Auditing/Federation of European Risk Management Associations (2010).

17 Vgl. Ruud und Kyburz (2014), S. 761.

18 Vgl. The Institute of Internal Auditors (2015a), S. 1 ff.

19 Vgl. The Institute of Internal Auditors (2013).

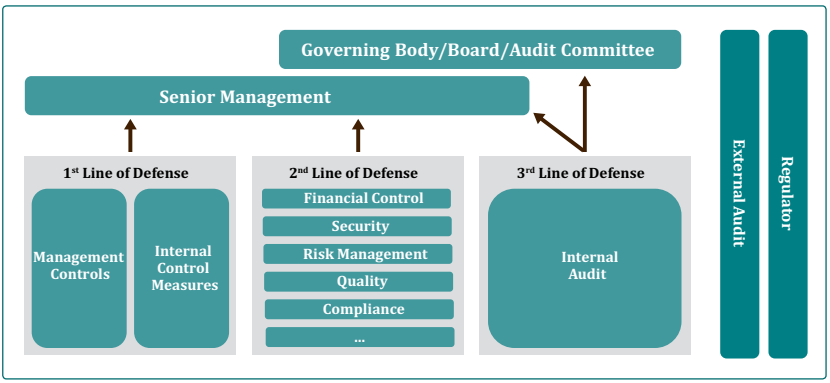


Abb. 10: Three-Lines-of-Defense-Modell

Bei der Auslegung des Modells ist es zentral, *«die wertschöpfenden Eigenschaften der Risiko- und Kontroll-Funktionen zu nutzen und keine rein abwehrende Erwartungshaltung zu entwickeln»*.[20] Folgt man dieser Argumentation, wäre der Gedanke der Verteidigung kritisch zu würdigen und die Bezeichnung *Kontrolllinien* als alternative Terminologie möglich. Das Modell hat die Wahrnehmung des Internen Audits gefördert, indem es das Interne Audit als dritte Linie separat hervorhebt und als wertschaffende Assurance-Aktivität stärker denn je auch visuell untermauert. Auch von den Unternehmen selbst wurde das Modell vielfach sehr positiv aufgenommen. Vor allem im Bankensektor, in dem die Einrichtung eines Internen Audits gemäss des *FINMA Rundschreibens 2017/01 Corporate Governance – Banken*[21] verpflichtend ist, hat das Modell starken Anklang gefunden. Auch für Organisationen, die nach Art. 728a OR gegenüber der Revisionsstelle die Existenz eines IKS nachweisen müssen, ist die Regelung der Verantwortlichkeiten analog zum Modell wertvoll und vorteilhaft.

Trotz der positiven Resonanz soll das Modell auch in der Zukunft nicht als statisch angesehen, sondern durchaus auch kritisch hinterfragt werden. Da es – wie jedes andere Modell – lediglich eine Vereinfachung der Wirklichkeit darstellt, ist die Ausgestaltung der Governance-Strukturen primär durch die unternehmensindividuellen Anforderungen zu bestimmen.

20 Vgl. Ruud und Kyburz (2014), S. 766.

21 Vgl. Eidgenössische Finanzmarktaufsicht FINMA (2017).

Ruud und Kyburz schlussfolgerten in diesem Zusammenhang, dass «*eine zu plakative Anwendung, d.h. ohne Rücksichtnahme auf unternehmensindividuelle Gegebenheiten […], verschiedene Gefahren einerseits für das Unternehmen als Ganzes, andererseits für die einzelnen Einheiten und deren Berufsstände*» mit sich bringen kann.[22] In Unternehmen, deren strukturelle und rechtliche Gegebenheiten keine drei voll ausgestalteten Linien nach Massgabe des Modells erfordern, würde eine zu modellgetreue Gestaltung der Strukturen möglicherweise zu Ineffizienzen führen. Geschäftsleitung und Verwaltungsrat stehen daher in der Verantwortung, die für ihr Unternehmen sinnvollste Lösung zu implementieren. Es zeigt sich, dass dies in der Praxis bereits häufig zum Tragen kommt. Zu beobachten ist in einigen Fällen, dass der Leiter des Internen Audits funktional an den CEO, CFO oder sogar an den Leiter der Rechtsabteilung – anstelle wie gefordert an den Verwaltungsrat – berichtet. Ausserhalb des Finanzsektors ist ausserdem gelegentlich eine Konvergenz zwischen zweiter und dritter Verteidigungslinie zu erkennen. Das bedeutet konkret, dass das Interne Audit teils oder ganz Aufgaben der zweiten Linie übernimmt.

Das IIA hat die Übernahme von Tätigkeiten der zweiten Verteidigungslinie im Rahmen des Practice Guides *Internal Audit and the Second Line of Defense*[23] frühzeitig adressiert. Es geht dabei auch auf Vorkehrungen hinsichtlich der Objektivität der Internen Auditoren ein, die bei der Ausführung von Tätigkeiten der zweiten Linie eventuell gefährdet sein könnte. Diese vom IIA vorgesehenen Massnahmen zur Erhaltung der Objektivität umfassen unter anderem:

- die Diskussion der einhergehenden Risiken mit der Geschäftsleitung und dem Verwaltungsrat
- die Akzeptanz und die Eigentümerschaft der Risiken durch die Geschäftsleitung
- die klare Definition und Zuteilung der Rollen und Verantwortlichkeiten
- die periodische Beurteilung der Berichterstattungslinien und Verantwortlichkeiten durch die Geschäftsleitung und den Verwaltungsrat

22 Vgl. Ruud und Kyburz (2014), S. 766.

23 Vgl. The Institute of Internal Auditors (2016).

- die Erfassung der Rollen des Internen Audits in der Geschäftsordnung des Internen Audits, der Internal Audit Charter
- die periodische unabhängige Beurteilung der Tätigkeiten des Internen Audits im Rahmen der zweiten Verteidigungslinie und der Wirksamkeit der Vorkehrungen hinsichtlich Unabhängigkeit, Objektivität und Assurance

Können Unabhängigkeit und Objektivität des Internen Audits auch unter Beachtung der vorgängigen Vorkehrungen nicht mehr gewährleistet werden, sollen die betreffenden Tätigkeiten anstelle des Internen Audits durch andere interne oder externe Stellen übernommen werden. In keinem Fall soll das Interne Audit folgende Tätigkeiten ausführen, welche vom IIA bereits *ex ante* formell ausgeschlossen wurden, da sie nicht mit der Definition und dem Mandat des Internen Audits vereinbar sind:

- Festlegung des Risikoappetits
- Eigentümerschaft oder das Management der Risiken
- Verantwortungsübernahme für das Rechnungswesen, die Geschäftsentwicklung oder für Tätigkeiten der ersten Verteidigungslinie
- Entscheidungen der Risikosteuerung im Namen der Geschäftsleitung
- Implementierung von respektive die Verantwortung für Risikomanagement- oder Governance-Prozesse(n)
- Assurance für Tätigkeiten der zweiten Verteidigungslinie, die das Interne Audit selbst erbracht hat

Die Übernahme von Tätigkeiten der zweiten Linie sollte generell nur von beschränkter Dauer sein. Andere Formen der Zusammenarbeit und der Koordination zwischen zweiter und dritter Linie wie beispielsweise gemeinsam durchgeführte Audits *(Integrated Audits)*, eine gemeinsam koordinierte Planung und Berichterstattung *(Process Integration)* oder der Informationsaustausch und die generelle Abstimmung der Tätigkeiten *(Alignment through Activities)* sind gemäss den Empfehlungen des IIA der vollen funktionalen Integration der beiden Linien vorzuziehen. Solange die Regelung der Verantwortlichkeiten die Erreichung der Unternehmensziele unterstützt und das Mandat des Internen Audits nicht einschränkt, sind die Darstellungen des Three-Lines-of-Defense-Modells als Empfehlung zu betrachten, von der bei Bedarf abgekehrt werden darf.

4.2 Implikationen für das Interne Audit

Die flexiblere Betrachtung des Modells hat bereits Einzug in die berufliche Praxis gefunden und wurde vom IIA wie zuvor erläutert im Rahmen eines Practice Guides adressiert. Da die Governance insbesondere im Nichtfinanzsektor als *Soft Law* vorgesehen ist, ist die Übernahme von Tätigkeiten der zweiten Linie durch das Interne Audit in diesen Unternehmen nicht unwahrscheinlich. Anders sieht es bei Finanzunternehmen aus, für welche strengere und verbindlichere Regelungen gelten und welche ihre Governance-Strukturen häufig genau nach dem Modell ausrichten. Für Banken und Versicherungen ab einer bestimmten Grösse ist eine relativ starke Orientierung an den Modellvorgaben daher weiterhin zu empfehlen und von einer Konvergenz zwischen zweiter und dritter Linie abzuraten.

5. Einordnung und Ausblick

In den letzten drei Dekaden hat das Interne Audit durch komplexere Risiken und zunehmende regulatorische Anforderungen stark an Bedeutung hinzugewonnen. Während es in den 1980er-Jahren häufig noch auf die Re-Performance beschränkt war, entwickelten sich in den Folgejahren nach und nach die drei Arbeitsgebiete Interne Steuerung und Kontrolle, Risikomanagement und Governance. Begleitet und vorangetrieben wurde die Entwicklung des Mandats jeweils durch die entsprechenden regulatorischen und berufsständischen Neuerungen. Heute sind die drei Arbeitsgebiete – lediglich in umgekehrter Reihenfolge zu ihrer geschichtlichen Entstehung – in IIA Standard 2100 *Art der Arbeiten* festgehalten. Vor allem im vergangenen Jahrzehnt hat sich zudem der Kerngedanke des Wertbeitrags, welcher seit 1999 in der Definition und seit 2015 auch in der Mission des Internen Audits verankert ist, noch stärker herauskristallisiert.[24]

24 Vgl. The Institute of Internal Auditors (2017).

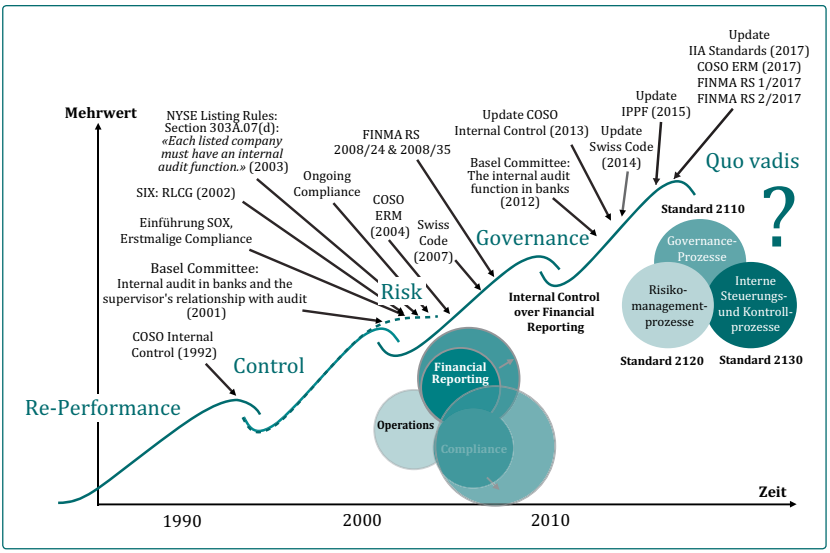


Abb. 11: Internal Audit – Quo vadis?

Das nun noch wertorientiertere Verständnis des Internen Audits fordert Verwaltungsrat und Geschäftsleitung dazu auf, aktuelle Trends auch übergreifender Natur zu verfolgen und deren potenzielle Auswirkungen auf die Arbeit ihres Internen Audits abzuwägen. Im Folgenden soll daher kurz auf die aktuellen Themen der strategischen Einbindung,[25] der Prüfung der Unternehmenskultur und auf den Einsatz von Data Analytics in den Prüfprozessen eingegangen werden, welche dazu beitragen können, dass das Interne Audit sein Mandat in den drei Kernarbeitsgebieten noch besser erfüllt und noch höhere Wertbeiträge für den Unternehmenserfolg leistet.

Die Tätigkeiten des Internen Audits im Gebiet Governance sehen vor, dass die strategischen Entscheide beurteilt und verbessert werden. Eine Voraussetzung dafür ist, dass das Interne Audit diejenigen Risiken, die mit bestimmten Strategien verbunden sind, kennt und die Führungsebene angemessen darauf hinweist. Gleichermassen ist die Abstimmung des Auditplans mit der Unternehmensstrategie eine Grundvoraussetzung dafür, dass das Interne Audit zur Zielerreichung beitragen kann. Das IPPF geht bereits an vielen Stellen auf strategische Aspekte ein, sodass Schnittmengen zwischen dem IPPF und der Leitidee des neuen COSO

25 Vgl. The Institute of Internal Auditors (2015b).

ERM zu erkennen sind. So weisen beide Standardsetter – IIA und COSO – auf ein eng mit der Unternehmensstrategie verknüpftes Verständnis von Governance, Risikomanagement und Interner Steuerung und Kontrolle hin.

Die Prüfung der Unternehmenskultur ist erst in den letzten Jahren als relevantes Governance-Thema in den Fokus gerückt, da die Schwerpunkte bislang eher in der finanziellen Berichterstattung oder in der Sicherstellung der Compliance – d.h. in den eher technischen Aspekten des Risikomanagements und der Internen Steuerung und Kontrolle – lagen. Die Unternehmenskultur gilt jedoch als sogenannter weicher Erfolgsfaktor, der die Zielerreichung indirekt über eine gesteigerte Mitarbeitermotivation, -loyalität und -integrität beeinflussen kann. In IIA Standard 2110 wird die Prüfung und Verbesserung der Unternehmenskultur mit dem Punkt zur Förderung ethisch angemessener Normen und Werte in der Organisation berücksichtigt.[26]

Bezug nehmend auf den möglicherweise häufigeren Einsatz von Data Analytics können viele Assurance-bezogene Tätigkeiten künftig gegebenenfalls von Software durchgeführt werden. Dadurch könnten sich die Effizienz und die Effektivität des Internen Audits erhöhen, da Ressourcen freigegeben werden und sich neue Schwerpunkte sowie neue Beratungsmöglichkeiten eröffnen. Daher ist es nicht unwahrscheinlich, dass sich das Verhältnis zwischen Assurance- und Consulting-Dienstleistungen etwas zugunsten von Beratung verschiebt. Die vom IIA und von vielen Praktikern befürwortete Wahrnehmung des Internen Audits als vertrauter Berater, als strategischer Partner auf Augenhöhe und als wertschaffende Aktivität könnte durch eine solche Verschiebung gefördert werden, da die Assurance-Tätigkeit in der Praxis noch mit der Konnotation der strengen Unternehmenspolizei assoziiert sein kann. Für typischerweise im Gebiet Governance angesiedelte innovative Themen, einschliesslich strategischer und kultureller Aspekte, ist die Anwendung von Software nur begrenzt möglich, da weiterhin ein hohes Mass an professionellem Urteilsvermögen notwendig ist.

26 Vgl. The Institute of Internal Auditors (2017).

Abschliessend ist festzuhalten, dass die drei in IIA Standard 2100[27] umschriebenen Arbeitsgebiete auch künftig für das Interne Audit relevant sein werden. Der ausschlaggebende Gedanke, der das Mandat des Internen Audits beeinflusst, ist der des *Wertbeitrags,* den das Interne Audit für das Unternehmen erbringt. Dieser kann traditionell durch Beurteilung und Verbesserung des IKS *(vgl. Kapitel 2),* durch Beurteilung und Verbesserung des Risikomanagements beispielsweise auf Basis des neuen COSO-ERM-Rahmenwerks *(vgl. Kapitel 3),* durch eine wirksame Gestaltung der Verantwortlichkeiten innerhalb der Three Lines of Defense *(vgl. Kapitel 4)* oder aber durch Berücksichtigung weiterer, aktueller Tendenzen *(vgl. obige Ausführungen)* erbracht und gefördert werden.

Literaturverzeichnis

Chrissis, M./Konrad, M./Shrum, S. (2009): CMMI® Richtlinien für Prozess-Integration, München 2009.

Committee of the Sponsoring Organizations of the Treadway Commission (2004): Enterprise Risk Management – Integrated Framework, Jersey City 2004.

Committee of the Sponsoring Organizations of the Treadway Commission (2013): Internal Control – Integrated Framework, Jersey City 2013.

Committee of the Sponsoring Organizations of the Treadway Commission (2017): Enterprise Risk Management – Aligning Risk with Strategy and Performance, Jersey City 2017.

Eidgenössische Finanzmarktaufsicht FINMA (2017): Rundschreiben 2017/1 Corporate Governance – Banken.

European Confederation of Institutes of Internal Auditing/Federation of European Risk Management Associations (2010): Guidance on the 8th EU Company Law Directive, article 41-2b.

Hunziker, S. (2018): Das neue COSO ERM Framework auf dem Prüfstand, in: Expert Focus 03/2018, S. 163–168.

International Organization for Standardization (2018): ISO 31000: Risk Management.

27 Vgl. The Institute of Internal Auditors (2017).

Ruud, F./Kyburz, A. (2014): Gedanken zum Three Lines of Defense Modell – Was ist mit Verteidigung gemeint? Analyse des Governance-Modells aus der Sicht des Internen Audits, in: Der Schweizer Treuhänder, 88(9), S. 761–766.

Ruud, F./Kyburz, A./Schramm, K. (2018): Das Interne Kontrollsystem in Schweizer Unternehmen ausserhalb des Finanzsektors.

The Institute of Internal Auditors (2013): IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, Altamonte Springs.

The Institute of Internal Auditors (2017): International Professional Practices Framework, Altamonte Springs, 2017.

The Institute of Internal Auditors (2015a): Leveraging COSO across the Three Lines of Defense, White Paper.

The Institute of Internal Auditors (2015b): Strategy-related auditing – Exploratory research on the consideration of strategic risk and organizational strategy in internal audits, Discussion Paper.

The Institute of Internal Auditors (2016): IIA Practice Guide: Internal Audit and the Second Line of Defense, Altamonte Springs.