Empfehlungen zur Optimierung des Zusammenwirkens von Interner Revision und Risikomanagement

Praxisleitfaden des Arbeitskreises
“Interne Revision und Risikomanagement”
des DIIR und der RMA

RMA Risk Management & Rating Association e.V.

DIIR Deutsches Institut für Interne Revision e.V.

Das optimale Zusammenspiel von Interner Revision und Risikomanagement - eine Anleitung zur praktischen Zusammenarbeit

Der regulatorische Rahmen steht nicht still: allein in diesem Jahr wurden mit dem FISG und dem StaRUG gleich zwei Governance-relevante Gesetzesinitiativen ratifiziert. Welche Auswirkungen hat dieses stark volatile regulatorische Umfeld eigentlich auf das Zusammenspiel von Revision und Risikomanagement - beides Funktionsbereiche, die sowohl gemeinsame als auch unterschiedliche Aufgaben zur Wahrung der Corporate Governance haben? Nur ein organisiertes Zusammenspiel von IR und RM ermöglicht ein zuverlässiges und effizientes Internes Überwachungssystem.

Vor diesem Hintergrund hat der Arbeitskreis “Interne Revision und Risikomanagement” des DIIR und der RMA, basierend auf dem gemeinsam entwickelten Positionspapier “Interne Revision und Risikomanagement - Empfehlungen zum Zusammenwirken (Mai 2020)”, Empfehlungen zur erfolgreichen Zusammenarbeit zwischen IR und RM entwickelt, die jüngst um konkrete Vorgehensweisen und Praxisleitfäden ergänzt worden sind.

Ausgangspositionen für die Zusammenarbeit innerhalb des Governance Systems

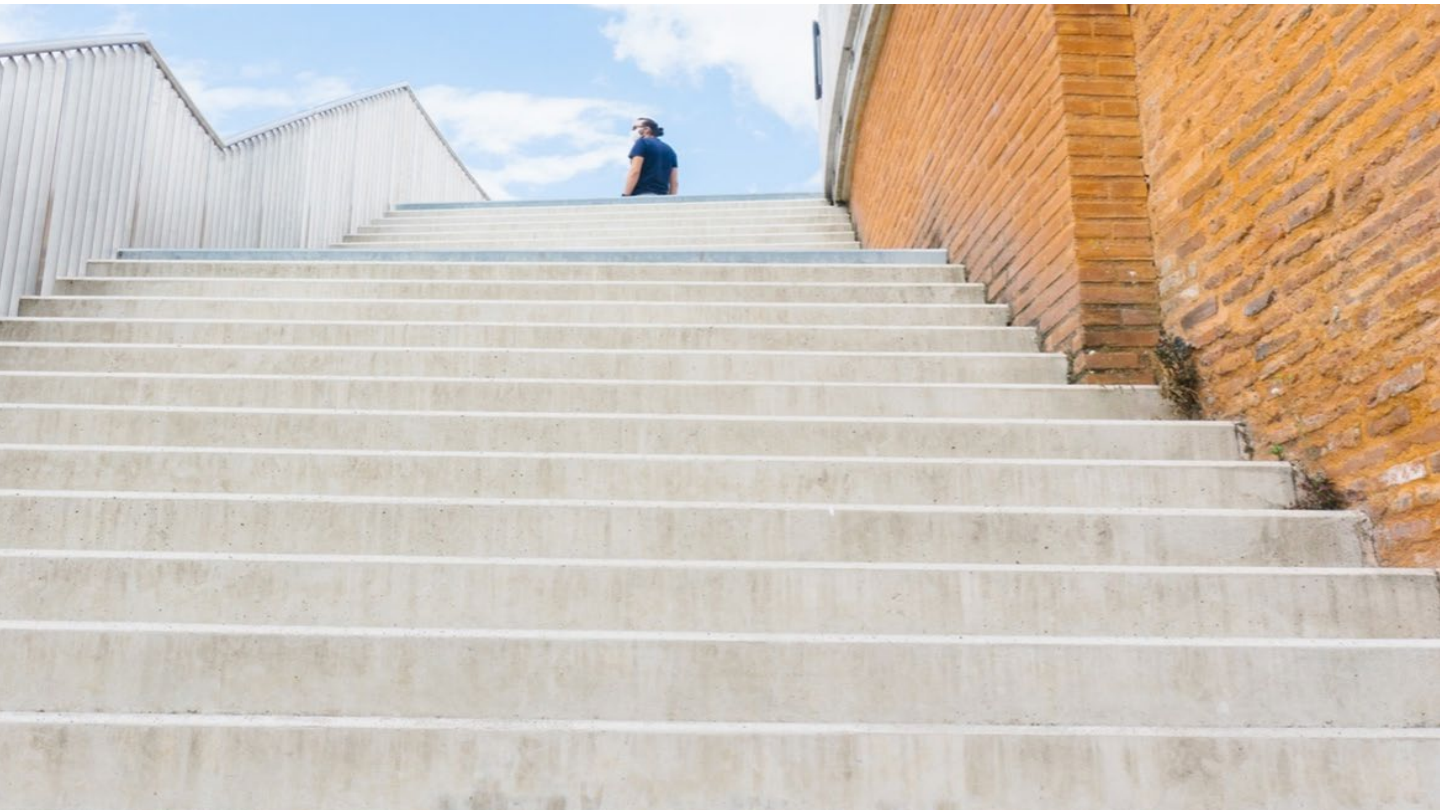
- Das Management von Risiken stellt zunächst eine generelle unternehmerische Aufgabe dar, die insbesondere Entscheidungsträgern im Management und in den Fachbereichen zukommt. Die Funktion Risikomanagement gestaltet hingegen das Risikomanagementsystem für das gesamte Unternehmen. Die Aufgaben schließen die Integration von Risikomanagement in die Geschäftsprozesse genauso wie die Etablierung einer Aufbauorganisation für das Risikomanagement ein.
- Nur ein angemessenes und wirksames Risikomanagementsystem kann folglich die Erreichung geplanter Unternehmensziele entsprechend unterstützen.
- Die Überwachung des Risikomanagementsystems erfolgt anhand von Prüfungen. Diese Prüfungen wiederum stellen auch eine Kernaufgabe der Internen Revision dar.
- Eine geeignet ausgestaltete, integrierte Zusammenarbeit zwischen der Internen Revision und dem Risikomanagement kann, vor dem Hintergrund eines immer komplexer und volatiler werdenden Unternehmensumfelds, zur zeitnahen Optimierung des Risikomanagementsystems beitragen.

Grundvoraussetzungen für eine Nutzung der Synergien

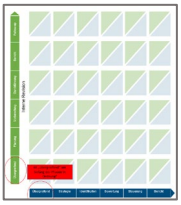
- Die Optimierung des Zusammenwirkens zwischen Interner Revision und Risiko-management beruht nicht nur auf der Identifikation von Synergien.
- Um entsprechende Synergie-Potentiale auch zu nutzen, sollte im Unternehmen grundsätzlich eine Bereitschaft zur Entwicklung eines integrierten GRC-Ansatzes vorliegen, konkret richtet sich das an
  - → das Top Management: „Tone of the Top“ und die Unterstützung, damit die Governance-Funktionen zielgerichtet zusammenarbeiten und Silos aufgebrochen werden können, sowie an
  - → die Governance-Funktionen: Schaffung von Transparenz zum Umgang mit Risiken.

Ferner sind Kompetenzen bei den Governance-Funktionen im Zusammenhang mit der Kommunikation und Offenheit für Veränderung notwendig:

- Bereitschaft zur Zusammenarbeit, Diskussion und Weiterentwicklung
- Kompromissbereitschaft
- Offenheit für die Sichtweise des anderen
- Vorhandensein eines gegenseitigen Einvernehmens zur
  - → Relevanz der Abstimmung zwischen den Bereichen und zur
  - → Notwendigkeit der Nutzung von Analysen zur Verbesserung bzw. Realisierung des integrierten GRC – Ansatzes
- vertrauenswahrende Kommunikation zwischen IR und RM
- prozessspezifische Agilität, d.h. das Verständnis, dass der IR- bzw. der RM-Prozess als Resultat des Informationsaustausches zwischen IR und RM im Einzelfall anders verlaufen kann oder grundsätzlich weiterentwickelt werden kann.

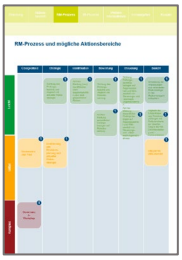


Nutzung/Erläuterung des Praxisleitfadens



- **Austausch-Matrix zur abteilungsübergreifenden Zusammenarbeit:** Anhand des Praxisleitfadens werden Aktionsbereiche für die Optimierung des Zusammenspiels identifiziert und entsprechende Handlungsempfehlungen konkretisiert, mit denen sich Synergien zwischen Revision und Risikomanagement realisieren lassen. Die Matrix zeigt die Aktionsbereiche, die Synergien oder Qualitätsvorteile mit Phasen der jeweils anderen Profession aufzeigen.

- **Ziele und Aufgaben:** Entlang des Prozesses von Revision bzw. Risikomanagement enthält jeder Prozessschritt die Beschreibung der mit dem jeweiligen Prozessschritt verbundenen Zielsetzungen.



- **Prozesse und Aktionsbereiche:** Um geeignete Aktionsbereiche vor dem Hintergrund des jeweils individuellen Unternehmenskontextes zu extrahieren, wird zunächst die Wahl der Funktion bzw. des Prozesses empfohlen, aus deren Perspektive primär das Zusammenspiel verbessert werden soll.

- **Aktionskarten:** Entlang des Prozesses von Revision bzw. Risikomanagement enthält jeder Prozessschritt patternartige Aktionskarten, die die jeweilige Vorgehensweise in strukturierter Form beschreiben. Jede Aktion wird entlang ihrer zugrundeliegenden Herausforderung (Motivation), eines fachlichen Anspruches an die Abteilung (Begründung) und der verfolgten Ziele beschrieben.
- Die Rubriken Push/Pull, Form, Teilnehmer und Häufigkeit helfen bei der Ausgestaltung der Aktion.

→ Push/Pull: Hier wird unterschieden, ob die ausführende Partei etwas einholen oder ausgeben bzw. anstoßen soll.

Form

→ Form: Bei der Aktion kann es sich um informelle Gespräche, Dokumenteneinsicht oder strukturierte Meetings handeln.

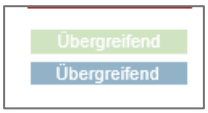
Teilnehmer

→ Teilnehmer: Hier werden neben Teilnehmern von Gesprächen auch Adressaten oder Quellen von Informationen genannt.

Häufigkeit

→ Häufigkeit: Wir unterscheiden insbesondere zwischen regelmäßigen und anlassbezogenen Aktivitäten, daneben wird eine Indikation für eine Wiederholungshäufigkeit bei regelmäßigen Aktivitäten gegeben.

Nutzung/Erläuterung des Praxisleitfadens



- **Phasen:** Neben Prozessschritt-spezifischen Ansätzen konnten auch prozessphasenübergreifende Elemente eines integrierten GRC-Ansatzes bzw. Aligned Assurance-Aktivitäten identifiziert werden, die das Zusammenwirken der Governance-Funktionen unterstützen können. Die beiden Aktionen "Governance Work-shop" und "Governance Jour Fixe" können von beiden Professionen vorangetrieben werden, idealerweise gemeinsam.

- **Schwierigkeit:** Der Schwierigkeitsgrad je Aktionskarte geht von einer Situation aus, in der die Zusammenarbeit mit der anderen Abteilung noch auszubauen ist bzw. neu begonnen werden soll. Jede erfolgreich umgesetzte, ggf. als Regel etablierte, Aktion erleichtert die Erschließung der nächstschwierigeren Handlungen.

- **Voraussetzungen**: Einige Aktionskarten setzen mehr voraus als andere Aktionskarten. In der Rubrik „Voraussetzungen" werden insbesondere solche Punkte genannt, die über die allgemeinen Voraussetzungen (Seite 3) hinausgehen.

- **Inhalt/Vorgehen:** Die Rubrik "Inhalt/Vorgehen" enthält einen Ablaufplan der jeweiligen Aktion. Beschreibt die Aktion ein Meeting, so ist an dieser Stelle auch eine Standardagenda zu finden.

- **Alternativen:** Unter Alternativen werden Abwandlungen der vorgestellten Aktion benannt. Teilweise stellen diese eine vereinfachte oder verkürzte Variante dar, die zum Beispiel dann zum Tragen kommen kann, wenn nicht alle Voraussetzungen der ausführlich beschriebenen Aktion erfüllt sind.

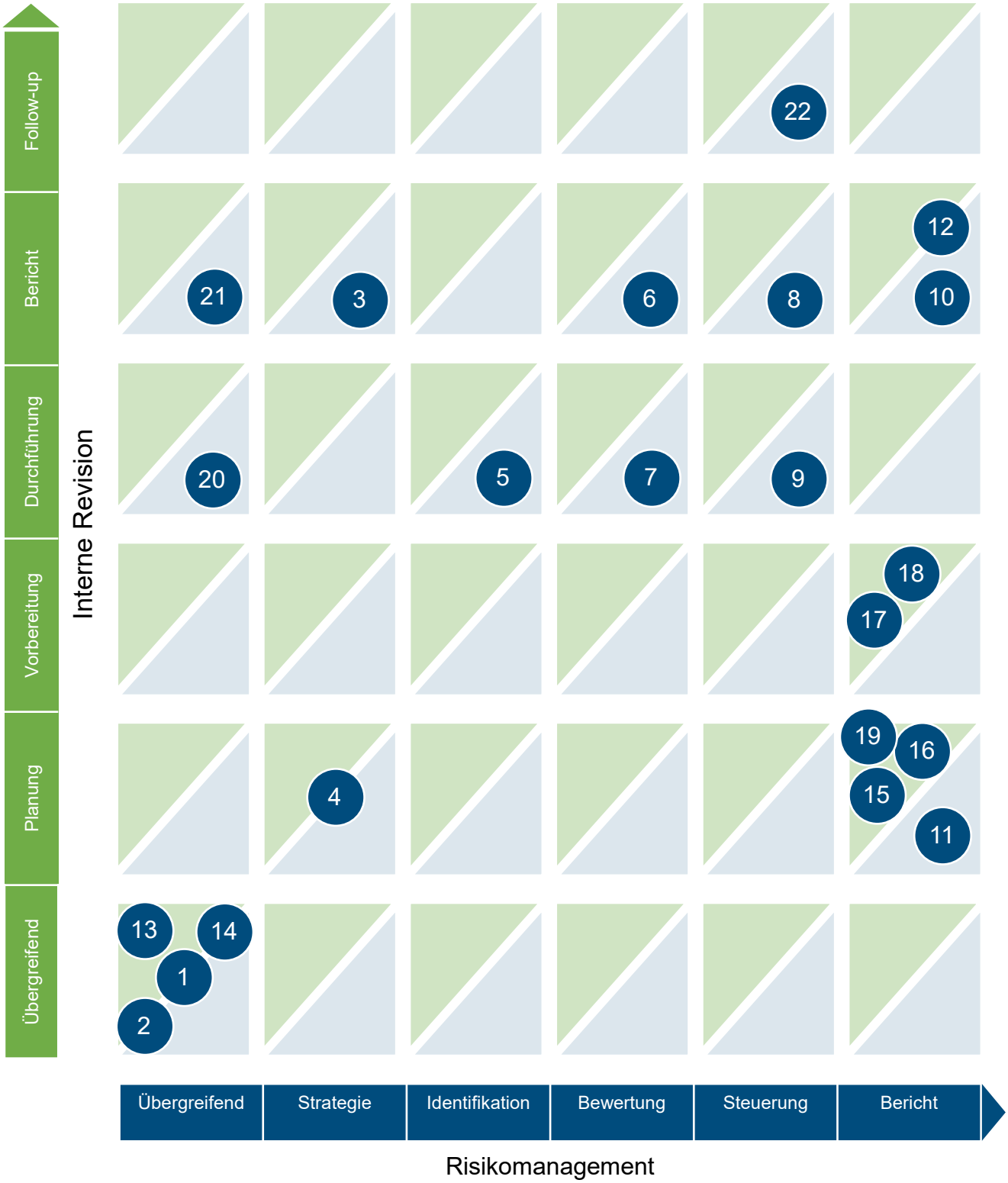
- **Empfehlungen:** Die Rubrik „Empfehlungen“ enthält bewährte Praxistipps zu der jeweiligen Aktion. Dabei kann es sich um Folgeaktionen oder Entscheidungshilfen handeln sowie beachtenswerte Details, die die Erfolgswahrscheinlichkeit der Aktion steigern helfen.

Die Aktionskarten verstehen sich als lebendige Erfahrungssammlung: Haben Sie bei der Erprobung der Aktionskarten Erkenntnisse gewonnen und Tipps entwickelt, die Sie mit anderen teilen möchten?

Geben Sie uns Bescheid – auch für neue Karten ist noch reichlich Platz vorhanden.

Viel Freude und Erfolg beim Ausprobieren!

Austausch-Matrix zur abteilungsübergreifenden Zusammenarbeit



RM-Prozess und mögliche Aktionsbereiche

Ziele und Aufgaben des Risikomanagements

- Beschreibung der Dokumentationsanforderungen im Hinblick auf Art und Umfang der Dokumente, Aufbewahrungsfristen
- Ausgestaltung des Berichtswesens: Adressaten der Berichte, Umfang und Frequenz der Berichte
- Definition der zu betrachtenden Einheiten und ggf. Clusterung z.B. im Hinblick auf die Risikoauswirkung
- Rollen und Verantwortlichkeiten im Risikomanagementprozess (insbesondere klare Trennung von Rollen)
- Festlegung und Beschreibung der Risikoarten
- Beschreibung wesentlicher und unwesentlicher Risiken
- Darstellung von Risikoauswirkungen auf das Unternehmen
- Darlegung der Methoden zur Risikoidentifikation
- Festlegung von Risikobewertungssystematik, insbesondere Begriffsdefinitionen für Schadens-ausmaß, Eintrittswahrscheinlichkeiten + Relevanzklassen, Zeithorizonte, Methoden der Risiko-quantifizierung, Berechnungsvorschriften des Gesamtrisikoumfangs und der Risikodeckungsmasse
- Festlegung des Umgangs mit Risiken, Risikobudgetierung (Limits und Selbstbehalte bei Risken)

RM-Prozess und mögliche Aktionsbereiche

	Übergreifend	Strategie	Identifikation	Bewertung	Steuerung	Bericht
Leicht		3 Sichtung Prüfungs-bericht und Abgleich mit aktueller Risiko-strategie	5 Ad-Hoc-Meldung (neu) identi-fizierter, stark abgeschwächter oder stark gewachsener Risiken	6 Sichtung Prüfungs-bericht und Abgleich mit Risiko-bewertung	8 Sichtung Prüfungsbericht bzgl. Ange-messenheit und Wirksamkeit von Steuerungs- und -überwachungs-maßnahmen	10 Umsetzung Anpassungen aus verän-derter Risiko-strategie in das Risiko-management system
				7 Ad-Hoc Meldung wesentlicher Findings bezogen auf Risikobe-wertung	9 Ad-Hoc Meldung wesentlicher Findings bzgl. Angemessenheit u. Wirksamkeit von Steuerungs- u. –überwachungs-maßnahmen	11 Abgleich Erkenntnisse aus Revisionsprüfungen mit Risikolandkarte zur Überführung in die RM-Berichter-stattung und -Kommunikation
Mittel	1 Governance Jour Fixe	4 Abstimmung von Revisions-planung und aktueller Risiko-strategie				12 Integrierter GRC-Bericht
Komplex	2 Governance Workshop					

Governance Workshop

1

Phasen

Übergreifend
Übergreifend

Push/Pull

✓ **Wechselseitig**
Pull RM
Push RM

Schwierigkeit

Leicht
Mittel
✔ **Komplex**

Kontakt

Gabriele Wieczorek

Motivation

- Steigerung der Qualität der Corporate Governance, insbesondere durch einen effektiveren und effizienteren Umgang mit Risiken über alle Governance-Funktionen hinweg
- Integriertes Risikomanagement

Begründung

- Verbesserung der Entscheidungsgrundlage gemäß der Business Judgement Rule
- Frühzeitige Erkennung bestandsgefährdender Entwicklungen nach KonTraG und StaRUG

Form

- Meeting

Teilnehmer

- IR, RM, Compliance, IKS, Vorstand

Häufigkeit

- Regelmäßig, ein- bis zweimal jährlich
- Frequenz abhängig vom (angestrebten) Reifegrad der integrierten Governance

Ziel

Etablierung einer integrierten Governance/ Combined Assurance

Koordination gemeinsamer Governance-Aktivitäten

Voraussetzungen

Zugriff und Austausch von (relevanten) Informationen

klares Commitment und Auftrag des Vorstand zur Integration verschiedener Governance-Funktionen

Inhalt/Vorgehen

Vorgehen
- Festlegung einer Organisationseinheit für die Durchführung des Workshops
- Terminabstimmung, Einladung mit Agenda und Dokumentation der Ergebnisse anhand Protokoll für Stakeholder
- Dokumentation und "Manifest" gemeinsamer Ergebnisse für den integrierten GRC-Ansatz

Inhalte
- Erarbeitung der Risikoterminologie
- Evaluation und Erarbeitung harmonisierter Elemente und Methoden im RMS
- Erarbeitung von Entscheidungsvorlagen

Alternativen

- abhängig vom Reifegrad können sowohl die Frequenz als auch die Inhalte in ihrer Detailtiefe sowie die Ziele angepasst werden, z.B. Variante 1: einmal jährlich findet ein Workshop zur Abstimmung des Reportings und/oder der Methodik zur Analyse und Steuerung der wesentlichen Risiken statt

Empfehlungen

- Durchführung eines Workshops unterstützt den Integrationsprozess in jedem Reifegrad.
- Formulierung der Zielsetzung eines Workshops vorab
- Stakeholder der Ergebnisse des Workshops können Fachbereiche, Vorstand sowie ein "Governance-Komitee" sein

Weitere mögliche Inhalte des Workshops:
- Entscheidungen über Integration weiterer Unternehmensbereiche/ Töchter und Beteiligungen
- Abstimmung gemeinsamer Governance-Themen
- Ableitung von Arbeitsgruppen für gemeinsame Governance-Themen
- Organisatorische/ prozessuale Abstimmung gemeinsamer Governance-Arbeitsschritte bzw. Abgrenzung einzelner Governance-Funktionen

Governance Jour Fixe

Phasen

Übergreifend
Übergreifend

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Schwierigkeit

Leicht
✔ **Mittel**
Komplex

Kontakt

Klaus Frech / Gabriele Wieczorek

Motivation

- Steigerung der Qualität der Corporate Governance

Begründung

- IPPF 2050 „Koordination und Vertrauen“: “Der Leiter der Internen Revision gibt Informationen an andere interne und externe Stellen weiter, die Prüfungs- und Beratungsleistungen erbringen und koordiniert die Aktivitäten mit diesen, damit eine angemessene Abdeckung erzielt und Doppelarbeiten vermieden werden.”

Form

- Meeting
- Umfang: 1-2h in Abhängigkeit der Frequenz

Teilnehmer

- IR, RM, Compliance, IKS
- jeweils Leiter und bis zu 2 Vertreter/ Mitarbeiter

Häufigkeit

- Regelmäßig, z. B. quartalsweise / monatlich / alle 2 Wochen

Ziel

Ausführlicher (informeller) Informationsaustausch und Identifikation wichtiger oder kritischer gemeinsamer Schnittstellenthemen

Gegenseitige Aktualisierung/Befragung zu dringenden Punkten/Themen

Aufdeckung und ggf. Behebung von Widersprüche in Berichten der Abteilungen

Harmonisierung von Reports/Entscheidungsvorlagen

Voraussetzungen

Zugriff und Austausch von (relevanten) Informationen

Inhalt/Vorgehen

Initiales Vorgehen
- Initiale Abstimmung einer organisierenden Funktion sowie eines regelmäßigen, festen Zeitfensters für Jour Fixe
- Initiale Festlegung einer Deadline für die Meldung von Themen für die Agenda und für den Versand der Agenda

Inhalte
- Abgleich und Diskurs der Berichte von IR und RM
- Diskurs zu aktuellen, aufkommenden Themen und organisatorischen / prozessualen Veränderungen
- Erstellung eines Protokolls

Alternativen

- GRC-Report, mit/ohne Vorstand

Empfehlungen

- Frühzeitige Planung von Terminen, z.B. idealerweise 4-5 Wochen vor Termin des Prüfungsausschusses bzw. ein regelmäßiger monatlicher Termin
- Versand der Dokumente vorab optional
- Jour Fixe stellt ein Element im integrierten Governance-Ansatz dar
- Nutzung des Jour Fixe auch zum informellen Austausch
- Etablierung einer kompatiblen Risikoterminologie und übersetzbaren Methodologie
- Die Inhalte des Protokolls können sich insbesondere auf abgestimmte Arbeitsschritten oder auf die Ausgestaltung der gemeinsamen Zusammenarbeit beziehen.

RM-Prozess und mögliche Aktionsbereiche

Übergreifend	Strategie	Identifikation	Bewertung	Steuerung	Bericht

Leicht

Mittel

Komplex

3 Sichtung Prüfungs-bericht und Abgleich mit aktueller Risiko-strategie

4 Abstimmung von Revisions-planung und aktueller Risiko-strategie

Die Grundlage des systematischen Umgangs mit unternehmerischen Risiken ist die Risikostrategie.

Ziele in der Phase "Strategie"

- Systematische Erfassung von Risiken
- Strukturierung von Risiken anhand einer Kategorisierung

Wie kann der RM-Prozessschritt “Strategie” mit Hilfe der IR verbessert werden?

Sichtung des Prüfungsberichts und Abgleich mit aktueller Risikostrategie

3

Phasen

Bericht
Strategie

Push/Pull

Wechselseitig
Push RM
✓ **Pull RM**

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Peggy Lilge

Motivation

- Berichterstattungspflicht der IR
- Sicherstellung vollständiger und zeitnaher Informationen an 2nd Line aus IR Prüfungen und Abgleich zwischen 2nd Line Funktionen über Informationsverarbeitung der von IR aufgezeigten Themen

Begründung

- DIIR Revisionsstandard Nr. 2
- IDW PS 981 Tz 58

Form

- Dokument: IR Prüfungsbericht
- Meeting: Durchsprache zwischen Revision und Risikomanagement

Teilnehmer

- Leitung IR
- Leitung RM
- Mitarbeiter RM

Häufigkeit

- Regelmäßig, Zusendung nach Fertigstellung oder nach Abschluss der Prüfung
- Anlassbezogen, im Falle von Ergebnissen, die eine unmittelbare Anpassung nötig machen

Ziel

Gebrauch von IR Prüfungsberichten als kontinuierliche Informationsquelle bzgl. Wirksamkeit des RMS

Nutzung der Erkenntnisse aus Revisions-prüfungen als Quelle für die Umsetzung der Risikostrategie in den Fachbereichen

Voraussetzungen

Vorliegen (finalisierter) Prüfungsberichte

Verständliche und adressatengerechte Aufbereitung der Berichtsform der IR

Existenz eines intern beschriebenen RM Prozesses mit entsprechenden Verant-wortlichkeiten zur Bearbeitung von IR Informationen

Inhalt/Vorgehen

- Erhalt der IR Berichte
- Sichtung der IR Informationen durch RM und Bewertung hinsichtlich Überführung in RM Prozesse
- Austausch mit Leitung IR zu abgeleiteten Anpassungs- bzw. Verbesserungsvorschlägen des RMS / Risikostrategie

Alternativen

- Initiierung der Durchsprache wesentlicher Prüfungsergebnisse durch IR
- softwareunterstützte Auswertung der Revisionsberichte
- Auswertung des IR Prüfungsberichts als dokumentierter Entscheidungsprozess

Empfehlungen

- Erarbeitung eines Vorschlags durch IR im Hinblick auf Verbesserungspotenziale für das RMS
- Harmonisierung der Timelines der Teilprozesse (grundsätzliches Thema für integrierten GRC – Ansatz)

Abstimmung von Revisionsplanung und aktueller Risikostrategie

4

Phasen

Planung
Strategie

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Motivation

– Integrierter GRC-Ansatz

Begründung

– DIIR Revisionsstandard Nr. 2: Prüfung des Risikomanagement-systems durch die Interne Revision: "Ausgehend von der [...] Risikostrategie folgen auf die Identifikation und Erfassung der Risiken und deren Analyse und Bewertung die Steuerung und Überwachung mit einer Rückkopplung zur Risikostrategie und ggf. deren Anpassung."

Schwierigkeit

Leicht
✔ **Mittel**
Komplex

Kontakt

Peggy Lilge

Form

– Meeting/ Dokument

Teilnehmer

- Revisionsleitung
- Leitung Risikomanagement

Häufigkeit

– Regelmäßig, ausgehend vom Planungszyklus der Revisionsplanung evtl. im Zuge von Risikostrategie – Checks

Ziel

Abgleich der Revisionsplanung und aktueller Risikostrategie

Harmonisierung der aktuellen Prüfungs-planung und neu hinzugekommenen oder aktuellen TOP Risiken des Unternehmens

Aufdeckung wesentlicher Diskrepanzen zwischen den inventarisierten oder einge-tretenen Risiken und der geplanten Revisionsprüfungen

Voraussetzungen

Zugriff und Austausch von (relevanten) Informationen

Inhalt/Vorgehen

– Vergleich der Revisionsplanung mit aktueller Risikoentwicklung
– Austausch mit Leitung IR zu abgeleiteten Anpassungs-/Verbesserungsvorschlägen des RMS / Risikostrategie (und einer Aktualisierung der Revisionsplanung im Umkehrschluss)

Alternativen

– entsprechend der internen Unternehmensprozesse

Empfehlungen

– Abgestimmte Timelines der Teilprozesse (grundsätzliches Thema für integrierten GRC – Ansatz)

RM-Prozess und mögliche Aktionsbereiche

	Übergreifend	Strategie	Identifikation	Bewertung	Steuerung	Bericht
Leicht			5 Ad-Hoc-Meldung (neu) identi-fizierter, stark abgeschwächter oder stark gewachsener Risiken			
Mittel						
Komplex						

Die Phase "Identifikation" umfasst die Risikoidentifikation und -erfassung.

Ziele der Phase "Identifikation"

- Systematische Erfassung von Risiken und deren Ursachen-Wirkungs-Beziehung
- Strukturierung von Risiken anhand einer Kategorisierung

Wie kann der RM-Prozessschritt “Identifikation” mit Hilfe der IR verbessert werden?

Ad-Hoc Meldung (neu) identifizierter, stark abgeschwächter oder stark gewachsener Risiken

Phasen

Durchführung
Identifikation

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Lars Düser/
Michael Hilser

Motivation

- Abwenden von Liquiditätsengpass, Schadenersatzpflicht o. Ä. durch frühzeitige Erkennung insbesondere stark gewachsener Risiken aus innerer oder äußerer Unternehmensumwelt
- Nachkommen der Veröffentlichungspflicht anderen Marktteilnehmern gegenüber, wie Gesellschafter bzgl. (bestands-gefährdender) Entwicklungen

Begründung

- Sicherstellung zeitnaher Informationen an 2nd Line aus IR Prüfungen zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen nach KonTraG und StaRUG
- Verbesserung der Entscheidungsgrundlage gemäß der Business Judgement Rule

Form

- Dokument: Vorabinformation, i.d.R. als IR Berichtsauszug oder in Ausnahmefällen dokumentierte Information über Email
- Ad-hoc-Meeting

Teilnehmer

- Leitung IR, Leitung RM, Risikoeigner
- involvierte Fachbereiche, Vorstand/ Geschäftsführung, Finanzen, ggf. Rechtswesen und Stakeholder

Häufigkeit

- Anlassbezogen
- bei bedeutende Feststellungen, z.B. bei neuen oder sich verstärkenden Risiken, deren Aktualität auf veränderte Rahmenbedingungen zurückzuführen ist

Ziel

Aktualität des Risikoinventars

Gewährleistung zeitnaher Etablierung von aktualisierter Risikohandhabungsstrategie

Gewährleistung eines kontinuierlichen Entscheidungsprozesses in RM zur Überführung der Informationen, insbesondere in RM Berichterstattung (oder z.B. ins RM-Komitee)

Voraussetzungen

Existenz eines RM intern beschriebenen Prozesses mit entsprechenden Verantwortlichkeiten zur Bearbeitung von wesentlichen Findings einschließlich Beschreibung der Handlungsoptionen

Inhalt/Vorgehen

- Sichtung der IR Teilinformationen durch RM
- Bewertung hinsichtlich Überführung in RM Prozesse
- Aktive Verarbeitung/umgehende Weitergabe seitens RM an relevante Stellen
- Ad-hoc-Abstimmung mit allen involvierten Bereichen und Funktionen durch RM zu notwendigen Verbesserungsmaßnahmen
- Ad-hoc Abstimmung mit IR bei offenen Fragen zu IR Informationen
- Dokumentation der erfassten Ad-Hoc-Ereignisse
- Überführung in die RM/IR-Berichterstattung

Alternativen

- Proaktive Ad-hoc-Meldung durch Prozessverantwortlichen
- Initiierung von Ad-hoc-Durchsprachen wesentlicher Findings durch die Revision
- Vorgehen zum Umgang mit Ad-hoc-Meldungen erfolgt als dokumentierter Entscheidungsprozess

Empfehlungen

- Meldung sollte durch IR nach Kenntnisnahme erfolgen
- Möglichkeit zur unterjährigen Verbesserung der Risikoinventarisierung und der Risikobewältigungsstrategie durch den Risikoeigner besteht
- Kompatible Risikoterminologie
- Etablierung eines regelmäßigen Austausches zwischen IR und RM und ggf. Erweiterung um weitere Teilnehmende wie CM

RM-Prozess und mögliche Aktionsbereiche

Übergreifend	Strategie	Identifikation	Bewertung	Steuerung	Bericht

Leicht

Mittel

Komplex

Die Phase "Bewertung" umfasst die Analyse und Bewertung von Risiken.

Ziele in der Phase "Bewertung"

- Analyse von Risiken und deren Auswirkungen auf die Unternehmensziele
- Qualitative und quantitative Risikobewertung, d.h. qualitativ beispielsweise zumindest nach Relevanz bis hin zur Risikoquantifizierung mit Hilfe von Wahrscheinlichkeitsverteilungen
- Erfassung von Wechselwirkungen zwischen Risiken
- Bestimmung des Gesamtrisikoumfangs – Risikoaggregation unter Redundanz-Gesichtspunkten

6 Sichtung Prüfungs-bericht und Abgleich mit Risikobe-wertung

7 Ad-Hoc Meldung wesentlicher Findings bezogen auf Risikobe-wertung

Wie kann der RM-Prozessschritt “Bewertung” mit Hilfe der IR verbessert werden?

Sichtung des Prüfungsberichts und Abgleich mit Risikobewertung

Phasen

Bericht
Bewertung

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Peter Rumpf

Motivation

Abgleich bzw. Sicherstellung der Vollständigkeit des Risikoinventars sowie relevanter (z.B. bestandsgefährdender) Risikobewertungen

Sicherstellung eines kontinuierlichen Verbesserungsprozesses für das RMS

Begründung

- Sicherstellung vollständiger und zeitnaher Informationen an 2nd Line aus IR Prüfungen und Abgleich zwischen 2nd Line Funktionen über Informationsverarbeitung der von IR aufgezeigten Themen
- Berichterstattungspflicht der IR
- DIIR Revisionsstandard Nr. 2

Form

- Dokument
- Meeting

Teilnehmer

- Leitung IR, Leitung und Mitarbeiter RM, Risikoeigner

Häufigkeit

- Regelmäßig, abhängig von Frequenz der Fertigstellung des Prüfungsberichts oder des Abschlusses der Prüfung

Ziel

Weitergabe der Erkenntnisse aus Revisionsprüfung zur Risikobewertung des Risikoeigners an RM

Information über identifizierte Schwachstellen bzw. Optimierungsmöglichkeiten

Voraussetzungen

Vorliegen (finalisierter) Prüfungsbericht

Verständliche und adressatengerechte Aufbereitung der Berichtsform

Existenz eines RM intern beschriebenen Prozesses mit entsprechenden Verantwortlichkeiten zur Bearbeitung von IR Informationen

Inhalt/Vorgehen

- Erhalt der IR Berichte
- Sichtung der IR Informationen durch RM und Bewertung hinsichtlich Überführung in RM Prozesse
- Zugehen auf Einheiten zur Abstimmung z.B. zur Anpassung der Risikobewertung
- Klärung von offenen Fragen mit IR
- Abgleich mit 2nd Line Funktionen IKS und CMS
- Austausch mit Rev.Ltg. zu abgeleiteten Anpassungs- bzw. Verbesserungsvorschlägen

Alternativen

- Initiierung einer Durchsprache wesentlicher Prüfungsergebnisse
- Softwaregestützte Auswertung der Revisionsberichte
- Auswertung des IR Prüfungsberichts erfolgt als dokumentierter Entscheidungsprozess

Empfehlungen

- Möglichkeit zur unterjährigen Verbesserung der Risikoinventarisierung und der Risikobewältigungsstrategie durch den Risikoeigner besteht
- Kompatible Risikoterminologie
- Etablierung eines regelmäßigen Austausches zwischen IR und RM und ggf. Erweiterung um weitere Teilnehmende wie CM
- Harmonisierung der Timelines der Teilprozesse abgestimmt (grundsätzliches Thema für integrierte Governance)
- Im Termin kann die Durchsprache zwischen Revision und Risiko-management z.B. zu Auffälligkeiten zur Beschreibung des Risikos, Datenbasis, Angemessenheit der Bewertungsmethodik bzw. stark abgeschwächter oder stark gewachsener Risiken erfolgen.
- Eine vollständige, angemessene und aktuelle Risikobewertung dient insbesondere der Ermittlung des unternehmerischen Gesamtrisikos.

Ad-Hoc Meldung wesentlicher Findings bezogen auf Risikobewertung

Phasen

Durchführung
Bewertung

Push/Pull

✓ **Push IR**

Motivation

- Zeitnahe Information von IR an RM von relevanten (v.a. bestandsgefährdenden) Risiken

Begründung

- Sicherstellung zeitnaher Informationen an 2nd Line aus IR Prüfungen zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen nach KonTraG und StaRUG
- Verbesserung der Entscheidungsgrundlage gemäß der Business Judgement Rule

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Peter Rumpf

Form

- Dokument: Vorabinformation, i.d.R. als IR Berichtsauszug oder in Ausnahmefällen dokumentierte Information über Email
- Ad-hoc Meeting: Durchsprache und Abstimmung des weiteren Vorgehens

Teilnehmer

- Leitung IR, Leitung RM, Risikoeigner, involvierte Fachbereiche, Vorstand/ Geschäftsführung, Finanzen, ggf. Rechtswesen und ggf. Stakeholder in Abhängigkeit von Art der Meldung

Häufigkeit

- Anlassbezogen

Ziel

Gewährleistung zeitnaher Etablierung von Verbesserungsmaßnahmen durch aktive Verarbeitung/Weitergabe seitens RM an relevante Stellen

Gewährleistung eines kontinuierlichen Entscheidungsprozesses in RM zur Überführung der Informationen, insbesondere in RM Berichterstattung (oder z.B. ins RM Komitee)

Voraussetzungen

Existenz eines RM intern beschriebenen Prozesses mit entsprechenden Verantwortlichkeiten zur Bearbeitung von wesentlichen Findings einschließlich Beschreibung der Handlungsoptionen (z.B. vereinfachte Entscheidungsmatrix und Berichtswegen)

Inhalt/Vorgehen

- Sichtung der IR Teilinformationen durch RM
- Bewertung hinsichtlich Überführung in RM Prozesse
- Aktive Verarbeitung/umgehende Weitergabe seitens RM an relevante Stellen
- Ad-hoc Abstimmung mit allen involvierten Bereichen und Funktionen durch RM zu notwendigen Verbesserungsmaßnahmen
- Ad-hoc Abstimmung mit IR bei offenen Fragen zu IR Informationen
- Dokumentation der erfassten Ad-Hoc-Ereignisse
- Überführung in die RM/IR-Berichterstattung

Alternativen

- Proaktive Ad-hoc Meldung durch Prozessverantwortlichen
- Initiierung von Ad-hoc Durchsprachen wesentlicher Findings durch die Revision
- Vorgehen zum Umgang mit Ad-hoc Meldungen erfolgt als dokumentierter Entscheidungsprozess

Empfehlungen

- Umsetzung des Berichtsweges kann durch definierte Schwellenwerte für eine Ad-Hoc Meldung unterstützt werden.
- Meldung durch IR erfolgt unmittelbar nach Kenntnisnahme

RM-Prozess und mögliche Aktionsbereiche

Übergreifend	Strategie	Identifikation	Bewertung	Steuerung	Bericht

Leicht

Mittel

Komplex

Die Phase "Steuerung" umfasst die Risikosteuerung und -überwachung.

Ziele in der Phase "Steuerung"

- Auswahl von angemessenen Risikobewältigungsstrategien - unter Berücksichtigung von Kosten und Nutzen sowie gesetzlicher Anforderungen sowie Anforderungen aus der Risikostrategie
- Überwachung der Risiken, z.B. mit Hilfe von Risikoindikatoren (Früh- oder Spätindikatoren) anhand definierter Schwellenwerten
- Überwachung der Wirksamkeit der Steuerungsmaßnahmen (Bemerkung: Hier besteht eine Schnittstelle zum Internen Kontrollsystem.)

8 Sichtung Prüfungsbericht bzgl. Angemessenheit und Wirksamkeit von Steuerungs- und Überwachungsmaßnahmen

9 Ad-Hoc Meldung wesentlicher Findings bzgl. Angemessenheit u. Wirksamkeit von Steuerungs- u. Überwachungsmaßnahmen

Wie kann der RM-Prozessschritt “Steuerung” mit Hilfe der IR verbessert werden?

Sichtung des Prüfungsberichtes bezogen auf Angemessenheit und Wirksamkeit von Steuerungs- und Überwachungsmaßnahmen

Phasen

Bericht
Steuerung

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Stefanie Klein

Motivation

- Das Risikomanagement soll umfassend über die Risikolage des Unternehmens informiert sein. Durch den Prüfungsansatz der IR erhält RM einen anderen Blickwinkel auf die Prozesse und dadurch neue Impulse zur Risikoidentifikation. Anhand der Berichte der IR ist die Wirksamkeit des eigenen Risikomanagement-systems zu erkennen.

Begründung

- Rolle von RM, gemäß Grundsätzen der ISO 31000 wie einer kontinuierlichen Verbesserung der RM-Organisation etc.
- Sicherstellung vollständiger und zeitnaher Informationen an 2nd Line aus IR Prüfungen und Abgleich zwischen 2nd Line Funktionen über Informationsverarbeitung der von IR aufgezeigten Themen
- DIIR Revisionsstandard Nr. 2

Form

- Dokument: IR Prüfungsbericht
- Meeting: Durchsprache zwischen Revision und Risikomanagement zu Auffälligkeiten zu Steuerungs- und Überwachungsmaßnahmen als Teil der Risikobewältigungsstrategie

Teilnehmer

- Leitung IR, Leitung und Mitarbeiter RM,
- Risikoeigner (oder generell Maßnahmenverantwortliche)

Häufigkeit

- Regelmäßig, abhängig von Frequenz der Fertigstellung des Prüfungsberichts oder des Abschlusses der Prüfung

Ziel

Aktualität des Risikoinventars

Gewährleistung zeitnaher Etablierung von aktualisierter Risikohandhabungsstrategie

Gewährleistung eines kontinuierlichen Entscheidungsprozesses in RM zur Überführung der Informationen, insbesondere in RM Berichterstattung (oder z.B. ins RM Komitee)

Voraussetzungen

Vorliegen (finalisierter) Prüfungsbericht

Verständliche und adressatengerechte Aufbereitung der Berichtsform
Existenz eines RM intern beschriebenen Prozesses mit entsprechenden Verantwortlichkeiten zur Bearbeitung von IR Informationen

Inhalt/Vorgehen

- Erhalt der IR Berichte
- Sichtung der IR Informationen durch RM und Bewertung hinsichtlich Überführung in RM Prozesse
- Zugehen auf Einheiten zur Abstimmung z.B. zur Anpassung der Risikobewertung
- Klärung von offenen Fragen mit IR
- Abgleich mit 2nd Line Funktionen IKS und CMS
- Austausch mit Rev.Ltg. zu abgeleiteten Anpassungs- bzw. Verbesserungsvorschlägen

Alternativen

- Initiierung einer Durchsprache wesentlicher Prüfungsergebnisse
- Softwaregestützte Auswertung der Revisionsberichte
- Auswertung des IR Prüfungsberichts erfolgt als dokumentierter Entscheidungsprozess

Empfehlungen

- Möglichkeit zur unterjährigen Verbesserung der Risikoinventarisierung und der Risikobewältigungsstrategie durch den Risikoeigner besteht
- Kompatible Risikoterminologie
- Etablierung eines regelmäßigen Austausches zwischen IR und RM und ggf. Erweiterung um weitere Teilnehmende wie CM
- Harmonisierung der Timelines der Teilprozesse abgestimmt (grundsätzliches Thema für integrierte Governance)

Ad-Hoc Meldung wesentlicher Findings bezogen auf Angemessenheit und Wirksamkeit von Steuerungs- und Überwachungsmaßnahmen

9

Phasen

Durchführung
Steuerung

Push/Pull

Wechselseitig
Push RM
✓ **Pull RM**

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Stefanie Klein

Motivation

- Durch das zeitnahe Informieren über wesentliche Findings hinsichtlich Steuerungs- und Überwachungsmaßnahmen kann RM schneller eingreifen und diese Maßnahmen gemeinsam mit dem Fachbereich optimieren, sodass die Risiken im Unternehmen wirksamer gesteuert sind.

Begründung

- Sicherstellung zeitnaher Informationen an 2nd Line aus IR Prüfungen zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen nach KonTraG und StaRUG
- Verbesserung der Entscheidungsgrundlage gemäß der Business Judgement Rule

Form

- Dokument: Vorabinformation, i.d.R. als IR Berichtsauszug oder in Ausnahmefällen dokumentierte Information über Email
- Ad-hoc Meeting: Durchsprache und Abstimmung des weiteren Vorgehen

Teilnehmer

- Leitung IR, Leitung RM,
- Risikoeigner, involvierte Fachbereiche,
- Vorstand/Geschäftsführung

Häufigkeit

- Anlassbezogen

Ziel

Gewährleistung zeitnaher Etablierung von Verbesserungsmaßnahmen durch aktive Verarbeitung/Weitergabe seitens RM an relevante Stellen

Gewährleistung eines kontinuierlichen Entscheidungsprozesses in RM zur Überführung der Informationen, insbesondere in RM Berichterstattung (oder z.B. ins RM Komitee)

Voraussetzungen

Existenz eines RM intern beschriebenen Prozesses mit entsprechenden Verantwortlichkeiten zur Bearbeitung von wesentlichen Findings einschließlich Beschreibung der Handlungsoptionen (z.B. vereinfachte Entscheidungsmatrix und Berichtswegen)

Inhalt/Vorgehen

- Sichtung der IR Teilinformationen durch RM
- Bewertung hinsichtlich Überführung in RM Prozesse
- Aktive Verarbeitung/umgehende Weitergabe seitens RM an relevante Stellen
- Ad-hoc Abstimmung mit allen involvierten Bereichen und Funktionen durch RM zu notwendigen Verbesserungsmaßnahmen
- Ad-hoc Abstimmung mit IR bei offenen Fragen zu IR Informationen
- Dokumentation der erfassten Ad-Hoc Ereignisse
- Überführung in die RM/IR-Berichterstattung HIER WEITER GW

Alternativen

- Proaktive Ad-hoc Meldung durch Prozessverantwortlichen
- Initiierung von Ad-hoc Durchsprachen wesentlicher Findings durch die Revision
- Vorgehen zum Umgang mit Ad-hoc Meldungen erfolgt als dokumentierter Entscheidungsprozess

Empfehlungen

- Definition von Schwellenwerten für die Angemessenheit und Wirksamkeit von Steuerungs- und Überwachungsmaßnahmen, anhand über Absatz einer Ad-hoc Meldung entschieden wird.
- Definition von Berichtswegen
- Meldung durch IR erfolgt unmittelbar nach Kenntnisnahme
- In Abhängigkeit der Art der Meldung (z.B. Bildung von Rückstellungen oder zur Einhaltung gesetzlicher Vorgaben) können Finanzen, Rechtswesen und ggf. auch Stakeholder involviert werden.

RM-Prozess und mögliche Aktionsbereiche

Übergreifend	Strategie	Identifikation	Bewertung	Steuerung	Bericht

Leicht

Mittel

Komplex

Die Phase "Bericht" umfasst die Dokumentation, Risikoberichterstattung und -kommunikation.

Ziele in der Phase "Bericht"

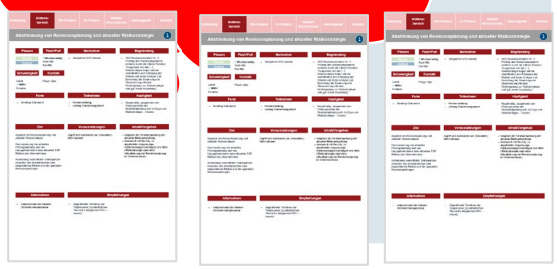
- Dokumentation der „operativen Umsetzung des Risikomanagementsystems“ in Form eines Risikomanagementhandbuchs
- Vorbereitung der Berichterstattung durch Prüfung des Risikoinventars/-registers auf Vollständigkeit, Plausibilität, Berücksichtigung von Wechselwirkungen
- Aufbereitung entscheidungsrelevanter Risikoinformationen, insbesondere über Maßnahmen zum Umgang mit Risiken und deren Wirksamkeit für die Stakeholder
- Schaffung einer Transparenz über die unternehmerische Risikosituation

10 Umsetzung Anpassungen aus veränderter Risikostrategie in das Risiko-management-system

11 Abgleich Erkenntnisse aus Revisionsprüfungen mit Risikolandkarte zur Überführung in die RM-Berichter-stattung und -kommunikation

12 Integrierter GRC-Bericht

Wie kann der RM-Prozessschritt “Bericht” mit Hilfe der IR verbessert werden?



Umsetzung der Anpassungen aus veränderter Risikostrategie in das Risikomanagementsystem

Phasen

Bericht

Bericht

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Peggy Lilge

Motivation

– Die Risikostrategie stellt die Basis des Umgangs mit Risiken im Unternehmenskontext dar. Um die Wirksamkeit des RMS im Sinne der Grundsätze der ISO 31000 wie einer kontinuierlichen Verbesserung der RM-Organisation etc. zu gewährleisten, resultiert eine Aktualisierung der Risikostrategie ggf. in Anpassungen an das RMS.

Begründung

– DIIR Revisionsstandard Nr. 2
– IDW PS 981 Tz 31

Form

– E-Mail durch RM, mit dem Ziel der Aktualisierung von RM-Dokumenten (z.B. Risikomanagementhandbuch, interne Richtlinie, Prozessbeschreibung)

Teilnehmer

- Leitung RM
- Leitung IR
- Risikoeigentümer

Häufigkeit

– Regelmäßig, im Anschluss an Strategie-Evaluation
– Anlassbezogen, Auslöser sind Ad-hoc Meldungen, die eine unmittelbare Anpassung nötig machen

Ziel

Aufrechterhaltung der Aktualität der Dokumentation der operativen Umsetzung des Risikomanagementsystems

Aufbereitung entscheidungsrelevanter Risikoinformationen
Vollständige und fehlerfreie Dokumentation des RMS

Gewährleistung der Wirksamkeit des RMS

Voraussetzungen

vorgelagerter Austausch zum Anpassungsbedarf der Risikostrategie aufgrund von Findings aus IR-Bericht mit Rev.Ltg. und weiteren relevanten Governance-nahen Bereichen (Compliance, Legal, …)

Inhalt/Vorgehen

– Identifikation von Erkenntnisse über eine veränderte Risikostrategie - aus Abgleich mit aktuellen Ergebnissen aus Revisionsprüfungen bzw. Revisionsplanung
– Aktualisierung der Dokumentation des RMS
– siehe dazu auch Aktionskarte zur Abstimmung der aktuellen Risikostrategie (RM-Prozessschritt Strategie, Aktionskarte S.1)

Alternativen

– Timing und Form je nach gegenseitigem Einvernehmen zur Relevanz der Abstimmung zw. den Bereichen und Notwendigkeit der Nutzung der Analysen zur Verbesserung / Erreichung des integrierten GRC – Ansatzes

Empfehlungen

– Anpassungen aus der Aktualisierung der Risikostrategie können z.B. die Berücksichtigung neuer Risikoverantwortlicher, neue wesentliche Risiken oder aktualisierte Bewertungsmethoden sein.

Abgleich der Erkenntnisse aus Revisionsprüfungen mit Risikolandkarte zur Überführung in die RM-Berichterstattung und -Kommunikation

Phasen

Planung
Bericht

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Peggy Lilge

Motivation

- Gewährleistung einer vollständigen und konsistenten Risikoberichterstattung, insbesondere zur frühzeitigen Kommunikation bestandsgefährdender Entwicklungen, auch durch Ad-hoc Meldungen

Begründung

- DIIR Revisionsstandard Nr. 2
- IDW PS 981 Tz 31 und A 27

Form

- Dokument: IR Prüfungsberichte
- Meeting (nach Bedarf): Durchsprache zwischen Revision und Risikomanagement

Teilnehmer

- Leitung IR
- Leitung RM
- Mitarbeiter RM

Häufigkeit

- Regelmäßig
- im Vorfeld von Risiko-Updates
- Abhängig von Frequenz der Fertigstellung des Prüfungsberichts oder des Abschlusses der Prüfung

Ziel

Unterstützt die Sicherstellung der Vollständigkeit und Aktualität der Risikolandkarte sowie der Vollständigkeit und Aktualität der Risikokommunikation und –dokumentation

Weitergabe der Erkenntnisse aus der Revisionsprüfung zur Risikohandhabung des Risikoeigners

Weitergabe von Schwachstellen bzw. Optimierungsmöglichkeiten durch IR

Voraussetzungen

Vorliegen (finalisierter) Prüfungsberichte

Verständliche und adressatengerechte Aufbereitung der Berichtsform

Existenz eines RM intern beschriebenen Prozesses mit entsprechenden Verantwortlichkeiten zur Bearbeitung von IR Informationen

Inhalt/Vorgehen

- Erhalt der IR Berichte
- Sichtung der IR Informationen durch RM zu den identifizierten Risiken hinsichtlich der Wesentlichkeit für RM
- Abgleich mit der aktuellen Risikolandkarte / Inventar
- Zugehen auf Einheiten zur Abstimmung bei Differenzen
- Klärung von offenen Fragen mit IR
- Abgleich mit 2nd Line Funktionen IKS und CMS

Alternativen

- Initiierung einer Durchsprache wesentlicher Prüfungsergebnisse
- Softwaregestützte Auswertung der Revisionsberichte
- Auswertung des IR Prüfungsberichts erfolgt als dokumentierter Entscheidungsprozess

Empfehlungen

- Idealerweise enthält ein Revisionsbericht ein separates Kapitel mit einer (komprimierten) ‚Risikoeinschätzung' der untersuchten Bereiche / Prozesse
- Prozessual verankerte Möglichkeit zur unterjährigen Verbesserung der Risikoinventarisierung und der Risikobewältigungsstrategie durch den Risikoeigner
- Kompatible Risikoterminologie
- Etablierung eines regelmäßigen Austausches zwischen IR und RM und ggf. Erweiterung um weitere Teilnehmende wie CM
- Harmonisierung der Timelines der Teilprozesse abgestimmt (im Sinne der integrierten Governance)

Integrierter GRC-Bericht

Phasen

Bericht
Bericht

Push/Pull

Wechselseitig
✓ **Push RM**
Pull RM

Schwierigkeit

Leicht
✓ **Mittel**
Komplex

Kontakt

Sebastian Bleich/
Peggy Lilge/
Gabriele Wieczorek

Motivation

- Steigerung der Qualität der Risiko-berichterstattung im Sinne einer integrierten Governance / Combined Assurance Ansatzes

Begründung

- Interne Vorgabe zur Berichterstattung und DIIR Nr. 1
- IPPF 2050 „Koordination und Vertrauen“
- IPPF 2060 „Berichterstattung an leitende Führungskräfte“
- Combined Assurance Ansatz

Form

- Auftakt-Meeting vor Dokumenterstellung
- Dokument

Teilnehmer

- Governance-Funktionen des Unternehmens, z.B. Revision, Risikomanagement, Compliance, IKS, Legal ggf. Leitung der Funktion

Häufigkeit

- Regelmäßig
- Definition der Frequenz durch Vorstand bzw. Aufsichtsrat

Ziel

Integrierte Darstellung der Gesamtrisikosituation auf Basis der Assurance-Aktivitäten der 2. und 3. Verteidigungslinien im Unternehmen.

Vermeiden von Information Overflow aufgrund multipler, uneinheitlicher und widersprüchlicher Berichterstattung

Integrierter GRC-Bericht als "Single Source of Truth"

Voraussetzungen

Auftrag vom Vorstand zur Erstellung eines integrierten GRC-Berichts

Definition der Governance-Funktionen, die zum GRC-Bericht beitragen

Einigung auf gemeinsame Darstellungsform für GRC-Bericht

Inhalt/Vorgehen

- Ausarbeitung Berichtsvorlage (mit jährlicher Evaluierung und Anpassung an interne und externe Anforderung)
- Auftakt-Meeting zur Vorstellung und Abstimmung der folgenden Inhalte
- Individuelle Arbeit am Dokument mit den abgestimmten Inhalten
- Abstimmung des vorfinalen Dokuments, ggf. mit einem Berichtsempfänger
- Befüllen des Berichts z. B. mit Statistiken, durchgeführten Assurance-Aktivitäten im Berichtszeitraum, wesentliche identifizierte Risiken gemäß einheitlicher Methodologie

Alternativen

- Jeder füllt den Bericht für sich aus und stimmt die Berichtsteile ab.

Empfehlungen

- Austausch zwischen den Governance-Funktionen hinsichtlich des jeweiligen Prüfungsscope, Risikobewertungsmethode, Risikodefinition/-sprache und Form der individuellen Berichterstattung z.B. im Governance-Workshop.
- Erarbeitung von Schnittmengen zwischen den Governance-Funktionen und Vereinheitlichung von Risikobewertungsmethoden und Risikosprache oder entsprechende „Übersetzung“ unterschiedlicher Ansätze auf einen gemeinsamen Nenner, z.B. im Governance-Workshop.
- Softwaregestützte Berichterstellung
- Reifegrad des GRC-Berichts hängt vom Reifegrad des integrierten GRC-Ansatzes sowie einer GRC-Strategie ab
- Abgleich mit Perspektive der Wirtschaftsprüfer im Hinblick auf die Erfüllung von Prüfungsvorgaben (inhaltliche Themen)

IR-Prozess und mögliche Aktionsbereiche

Ziele und Aufgaben der Internen Revision

- Prüfungs- und Beratungstätigkeiten, die auf die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse ausgerichtet sind
- Überprüfung der Funktionsfähigkeit und Wirksamkeit des Risikomanagements im Ganzen oder im Einzelfall. Gemäß dem DIIR-Revisionsstandard Nr. 2 gehört zur Funktionsfähigkeit, dass:
  - → wesentliche Risiken erkannt und bewertet werden,
  - → angemessene Risikomaßnahmen, die mit der Risikoakzeptanz der Organisation im Einklang stehen, ergriffen werden und
  - → wesentliche risikobezogene Informationen erfasst und rechtzeitig in der Organisation kommuniziert werden, sodass es Mitarbeitenden, Führungskräften und Geschäftsleitung bzw. Überwachungsorgan möglich ist, ihren Verantwortlichkeiten gerecht zu werden.
- Vorgehen nach dem Prinzip der Risikoorientierung:
  - → In allen Phasen des Revisionsprozesses sind Entscheidungen (z.B. über das weitere Prüfungsvorgehen) und Bewertungen (z.B. von vorgefundenen Auffälligkeiten) auf Basis von Risikoeinschätzungen vorzunehmen.
  - → Informationen, Expertise und Verfahren aus dem Risikomanagement (-Prozess) können daher den Revisionsprozess als solchen auch direkt unterstützen.

IR-Prozess und mögliche Aktionsbereiche

	Übergreifend	Planung	Vorbereitung	Durchführung	Bericht	Follow-up
Leicht	13 Teilnahme Risiko-ausschuss/ -komitee	15 Jahres-interview zur Erhebung von Risiken	17 Detail-Sichtung des Risiko-inventars hinsichtlich Prüfungs-auftrag	19 Expertise bei Bewertung von Risiken einholen		22 Information über aktuellen Umsetzungs-grad der Maßnahmen
Leicht	14 Regelmäßige unterjährige Jour-Fixe mit dem Konzern-Risiko-manager	16 Dokumenten-basierter Risikoab-gleich mit Risiko-management		20 Ad-hoc-Meldung identifizierter Risiken durch IR		
Mittel	1 Governance Jour Fixe		18 Stakeholder Feedback: Prüfungs-spezifisches Interview mit verantwort-lichem Risiko-manager		21 Verteilung / Berichts-verteiler Revisions-berichte	12 Integrierter GRC-Bericht
Komplex	2 Governance Workshop					

Governance Workshop

Phasen

Übergreifend
Übergreifend

Push/Pull

✓ **Wechselseitig**
Pull RM
Push RM

Schwierigkeit

Leicht
Mittel
✔ **Komplex**

Kontakt

Gabriele Wieczorek

Motivation

- Steigerung der Qualität der Corporate Governance, insbesondere durch einen effektiveren und effizienteren Umgang mit Risiken über alle Governance-Funktionen hinweg
- Integriertes Risikomanagement

Begründung

- Verbesserung der Entscheidungsgrundlage gemäß der Business Judgement Rule
- Frühzeitige Erkennung bestandsgefährdender Entwicklungen nach KonTraG und StaRUG

Form

- Meeting

Teilnehmer

- IR, RM, Compliance, IKS, Vorstand

Häufigkeit

- Regelmäßig, ein- bis zweimal jährlich
- Frequenz abhängig vom (angestrebten) Reifegrad der integrierten Governance

Ziel

Etablierung einer integrierten Governance/ Combined Assurance

Koordination gemeinsamer Governance-Aktivitäten

Voraussetzungen

Zugriff und Austausch von (relevanten) Informationen

klares Commitment und Auftrag des Vorstand zur Integration verschiedener Governance-Funktionen

Inhalt/Vorgehen

Vorgehen
- Festlegung einer Organisationseinheit für die Durchführung des Workshops
- Terminabstimmung, Einladung mit Agenda und Dokumentation der Ergebnisse anhand Protokoll für Stakeholder
- Dokumentation und "Manifest" gemeinsamer Ergebnisse für den integrierten GRC-Ansatz

Inhalte
- Erarbeitung der Risikoterminologie
- Evaluation und Erarbeitung harmonisierter Elemente und Methoden im RMS
- Erarbeitung von Entscheidungsvorlagen

Alternativen

- abhängig vom Reifegrad können sowohl die Frequenz als auch die Inhalte in ihrer Detailtiefe sowie die Ziele angepasst werden, z.B. Variante 1: einmal jährlich findet ein Workshop zur Abstimmung des Reportings und/oder der Methodik zur Analyse und Steuerung der wesentlichen Risiken statt.

Empfehlungen

- Durchführung eines Workshops unterstützt den Integrationsprozess in jedem Reifegrad.
- Formulierung der Zielsetzung eines Workshops vorab
- Stakeholder der Ergebnisse des Workshops können Fachbereiche, Vorstand sowie ein "Governance-Komitee" sein

Weitere mögliche Inhalte des Workshops:
- Entscheidungen über Integration weiterer Unternehmensbereiche/ Töchter und Beteiligungen
- Abstimmung gemeinsamer Governance-Themen
- Ableitung von Arbeitsgruppen für gemeinsame Governance-Themen
- Organisatorische/ prozessuale Abstimmung gemeinsamer Governance-Arbeitsschritte bzw. Abgrenzung einzelner Governance-Funktionen

Governance Jour Fixe

Phasen

Übergreifend
Übergreifend

Push/Pull

✓ **Wechselseitig**
Push RM
Pull RM

Schwierigkeit

Leicht
✔ **Mittel**
Komplex

Kontakt

Klaus Frech / Gabriele Wieczorek

Motivation

- Steigerung der Qualität der Corporate Governance

Begründung

- IPPF 2050 „Koordination und Vertrauen“: “Der Leiter der Internen Revision gibt Informationen an andere interne und externe Stellen weiter, die Prüfungs- und Beratungsleistungen erbringen und koordiniert die Aktivitäten mit diesen, damit eine angemessene Abdeckung erzielt und Doppelarbeiten vermieden werden.”

Form

- Meeting
- Umfang: 1-2h in Abhängigkeit der Frequenz

Teilnehmer

- IR, RM, Compliance, IKS
- jeweils Leiter und bis zu 2 Vertreter/ Mitarbeiter

Häufigkeit

- Regelmäßig, z. B. quartalsweise / monatlich / alle 2 Wochen

Ziel

Ausführlicher (informeller) Informationsaustausch und Identifikation wichtiger oder kritischer gemeinsamer Schnittstellenthemen

Gegenseitige Aktualisierung/Befragung zu dringenden Punkten/Themen

Aufdeckung und ggf. Behebung von Widersprüche in Berichten der Abteilungen

Harmonisierung von Reports/Entscheidungsvorlagen

Voraussetzungen

Zugriff und Austausch von (relevanten) Informationen

Inhalt/Vorgehen

Initiales Vorgehen
- Initiale Abstimmung einer organisierenden Funktion sowie eines regelmäßiges, festes Zeitfenster für Jour Fixe
- Initiale Festlegung einer Deadline für die Meldung von Themen für die Agenda und für den Versand der Agenda

Inhalte
- Abgleich und Diskurs der Berichte von IR und RM
- Diskurs zu aktuellen, aufkommenden Themen und organisatorischen / prozessualen Veränderungen
- Erstellung eines Protokolls

Alternativen

- GRC-Report, mit/ohne Vorstand

Empfehlungen

- Frühzeitige Planung von Terminen, z.B. idealerweise 4-5 Wochen vor Termin des Prüfungsausschusses bzw. ein regelmäßiger monatlicher Termin
- Versand der Dokumente vorab optional
- Jour Fixe stellt ein Element im integrierten Governance-Ansatz dar
- Nutzung des Jour Fixe auch zum informellen Austausch
- Etablierung einer kompatiblen Risikoterminologie und übersetzbaren Methodologie
- Die Inhalte des Protokolls können sich insbesondere auf abgestimmte Arbeitsschritten oder auf die Ausgestaltung der gemeinsamen Zusammenarbeit beziehen.

Teilnahme Risikoausschuss/-komitee

Phasen

Übergreifend

Übergreifend

Push/Pull

✓ **Wechselseitig**
Push IR
✓ **Pull IR**

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Klaus Frech

Motivation

- Austausch auf Top-Level-Ebene zur Risikolage und damit relevante Informationen für die Revision (Planung, mehrjährige oder auch unterjährige Planung)
- Fehlen relevanter und aktueller Risikoinformationen über nicht kürzlich geprüfte Bereiche

Begründung

- Standard 2050: Coordination & Reliance (Abstimmung und Zusammenarbeit)
- Practice Advisory 2050-2 Assurance Map / Abs 6 (Koordination, Abgleich)

Form

- Meeting
- Umfang bis 2 Stunden

Teilnehmer

- Vertreter des Vorstands, RM, Vorsitzende der Geschäfts- und Funktionaleinheiten und wesentlichen Tochtergesellschaften
- Revisionsvertreter optional

Häufigkeit

- Regelmäßig, quartalsweise

Ziel

Risikomanagement: Verabschiedung des Quartals-Chancen-/Risikoberichts sowie Anpassung durch Ergänzung neuer Risiken und Aktualisierung der Risikolage aus Top-Down-Sicht

Revision: Informationen / Einschätzung des Seniors und Top-Managements aus erster Hand erfahren

Voraussetzungen

Die Revision sollte mindestens Protokolleinsicht erhalten.

Inhalt/Vorgehen

- Top-Down-Diskussion von relevanten Risiken (im Gegensatz zur Bottom-Up Sammlung der Risiken über den Standard-RM-Prozess) entlang Top-Level-Risiko-Kategorien
- Nebenziel: Diskurs /Verbesserung des Risikomanagement-Prozesses
- Teilnahme IR als eher passiver Zuhörer und Berater - i.d.R. kein Stimmrecht

Alternativen

- Ggf. reine Protokolleinsicht anstelle der aktiven Teilnahme im Termin.

Empfehlungen

- Dokumente optional vorher zusenden
- RM lädt ein
- Konkrete Fragestellungen im Vorfeld zur Vorbereitung stellen oder als TOP auf Agenda nehmen

Regelmäßige unterjährige Jour-Fixe mit dem Konzern-Risikomanager

Phasen

Übergreifend

Übergreifend

Push/Pull

✓ **Wechselseitig**
Push IR
Pull IR

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Markus Silber

Motivation

- Möglichkeit gegenteiliger oder unvollständiger Sichten, Vorgehensweisen und/oder Doppelarbeiten.

Begründung

- IPPF 2010: Die Planung muss risikoorientiert sein.
- Standard 2050: Coordination & Reliance (Abstimmung und Zusammenarbeit)
- Practice Advisory 2050-2 Assurance Map / Abs 6 (Koordination, Abgleich)

Form

- Telefonat/Meeting
- Festes Meeting zu einem, mit dem RM abgestimmten, regelmäßigen Termin
- Dauer: z.B. quartalsweise 1h

Teilnehmer

- Leitung IR und RM bzw. jeweils ein, von der Leitung bestimmter, Vertreter

Häufigkeit

- Regelmäßiger Termin der mittels Terminserie festgelegt wird. (z.B. quartalsweise)

Ziel

Regelmäßiger Austausch zu aktuellen Risikoinformationen sowie relevanten Aktivitäten und (methodischen) Änderungen (s. hierzu auch Governance Jour-Fixe)

Integration von Informationen des Risikomanagements bei der Jahresplanung und Planung der Schwerpunkte der Revisionsprojekte (s. hierzu auch Jahresinterview zur Erhebung der Risiken)

Voraussetzungen

Revisionsleitung muss Zugang zu den Informationen des Risikomanagements haben. Vermerk in der Audit Charta

Meeting vorbereiten, vorab Fragen und Themen sammeln

Inhalt/Vorgehen

- Besprechung des aktuellen Risikoberichts und ggf. jeweilige Arbeitsschwerpunkte
- Identifikation potenzieller Revisionsfelder

Alternativen

- Themenbezogene Einladung von Risikomanagement-Spezialisten in Revisions-Jour-Fixe (oder umgekehrt)

Empfehlungen

IR-Prozess und mögliche Aktionsbereiche

Übergreifend	Planung	Vorbereitung	Durchführung	Bericht	Follow-up

Leicht

Mittel

Komplex

15 Jahres-interview zur Erhebung von Risiken

16 Dokumenten-basierter Risikoab-gleich mit Risiko-management

Ziele der Phase "Planung"

- Aktualisierung eines Audit Universe mit dem Ziel der vollständigen Erfassung aller unternehmensrelevanten Risiken unter Einbezug aller zuvor systematisch eingeholten aktuellen Informationen über die Prüfungsgebiete (bspw. auch über Jahresinterviews (s.o.)

- Erstellung einer risikoorientierten Jahresplanung mit dem Ziel des risikoadäquaten Ressourceneinsatzes:
  - → Überprüfung der Methodik der Risikobewertung
  - → Systematische Risikobewertung der Prüfgebiete basierend auf einem objektiven Risikobewertungsverfahren (bspw. Scoringverfahren) unter Einbezug aller zuvor systematisch eingeholten aktuellen Informationen über die Prüfungsgebiete (bspw. auch über Jahresinterviews (s.o.))
  - → Berechnung der Nettoressourcen für Prüfungs- und Beratungsleistungen
  - → risikoorientierte Verteilung der Nettoressourcen auf Prüfgebiete und Projekte
  - → ggf. Einplanung des Zukaufs externer Ressourcen bei Unterdeckungen
- Erstellung einer darauf aufbauenden Zeit-, Personaleinsatz-, Ausbildungs- und Personalentwicklungsplanung
- Erstellung einer kommentierten Genehmigungs-/Entscheidungsvorlage zur Jahresplanung für die Unternehmensleitung (Vorstand/Geschäftsführung)

Wie kann der IR-Prozessschritt "Planung" mit Hilfe des RM verbessert werden?

Jahresinterview zur Erhebung von Risiken

Phasen

Planung
Bericht

Push/Pull

Wechselseitig
Push IR
✓ **Pull IR**

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Bernhard Geiger

Motivation

- Vermeidung von Lücken in der Risikoschau auf beiden Seiten (IR/RM)
- Vermeidung von Doppelarbeiten
- ggf. unvollständige oder nicht aktuelle Informationslage zu Risiken / falsch priorisierte Prüfungsplanung

Begründung

- IPPF 2010 – Der Leiter der Internen Revision muss einen risikoorientierten Prüfungsplan erstellen
- IPPF 2050: Coordination & Reliance (Abstimmung und Zusammenarbeit)
- Practice Advisory 2050-2 Assurance Map / Abs 6 (Koordination, Abgleich)

Form

- Festes turnusmäßiges Jahresmeeting auf Leitungsebene
- ggf. mit Breakouts/ Vertiefungsworkshops
- Dauer ca. 2 Stunden (ggf. mehrfach)

Teilnehmer

- IR und RM - jeweils Leiter und Mitarbeiter nach Bedarf
- ggf. Experten für wichtige Themen je nach Agenda

Häufigkeit

- Regelmäßig, i.d.R. turnusmäßig, meist jährlich, im Rahmen der Planungsphase
- Anlassbezogen ggf. bei stärkeren Anpassungen des Audit Universe oder der Risikoinventarliste

Ziel

Ausführlicher bilateraler Austausch von Risikoinformationen

Diskurs aktueller Risikoentwicklungen
- Vervollständigung Audit Universe/Risk Assessment mit Blick auf das nächste Jahr
- Abgleich der Priorisierung (d.h. grobe Abstimmung und möglichst Common Sense) über die Bewertung/Einschätzung der Risiken sowie ihrer Beziehung untereinander
- Absicherung/Qualitätssicherung

Voraussetzungen

Kompatible Risikoterminologie

Strukturierte Vorbereitung/Unterlagen, z.B.:
- Aktuelles Prüfungsuniversum
- Draft 1 neue Jahresplanung i.v.m. Mehrjahresplanung
- Fragenliste (z.B. zu größeren Veränderungen, unklaren Einschätzungen, Rankings und Gewichtungen)

Verbindlichkeit des Vereinbarten: Austausch entsprechender Dokumente im Nachgang des Meetings (bspw. Draft 2 zur Prüfungsplanung; aktualisiertes Risikoinventar, etc.)

Inhalt/Vorgehen

- Ausführlicher bilateraler Austausch von Risikoinformationen
- insbesondere mit Fokus auf die geplanten oder möglichen Veränderungen im internen oder externen Risikoumfeld des Unternehmens (z.B. Produkte/Märkte/Gesetze/ Organisation/Personal etc.)
- Vorgehen entlang der Prüfungsuniversums bzw. des Entwurfs des Prüfungsplans

Alternativen

- Möglicher Einbezug von Compliance in einer Dreierrunde, erfordert jedoch einen noch höheren Reifegrad und Erfahrungspraxis solcher Abstimmgespräche

Empfehlungen

- Dokumentierte Risiken erfüllen bestimmte formale Hürden; gezielt hinterfragen, welche Themen und Entwicklungen ggf. darüber hinausgehen
- In besonderen Unternehmensphasen (bspw. vor und nach Fusionen; bei sehr jungen Unternehmen wie bspw. Start-up-Unternehmen) bieten sich kürzere Zeitabstände für die Planung an (bspw. Halbjährlich/vierteljährlich), jedoch abhängig von Vorarbeiten ("Anlässen") auf IR- und RM-Seite

Dokumentenbasierter Risikoabgleich mit RM

Phasen

Planung
Bericht

Push/Pull

Wechselseitig
Push IR
✓ **Pull IR**

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Sebastian Bleich

Motivation

- Herausforderung: unvollständige Information oder widersprechende Sichtweisen

Begründung

- IPPF 2010 “Planung” muss risikoorientiert sein und enthält relevante Informationen von Führungskräften, der Geschäftsleitung bzw. des Überwachungsorgans

Form

- Sichtung aktueller Risikobericht, Risikoregisters/-inventar etc., inkl. Ad-hoc Meldungen
- Optional, falls zusätzlich notwendig: Telefonat/Meeting mit Risikomanager bei Unklarheiten

Teilnehmer

- Revisionsleitung bzw. Verantwortliche für Revisionsplanung
- Ggf. Risikomanager

Häufigkeit

- Regelmäßig, mindestens jährlich oder häufiger in Abhängigkeit der Frequenz der übergeordneten Prüfungsplanung

Ziel

Risikoinformationen vom Risikomanagement werden in der Jahresplanung und im Audit Universe berücksichtigt

Prüfungsplanung berücksichtigt alle wesentlichen Informationen, um Risiken zu identifizieren und zu priorisieren.

Voraussetzungen

Revisionsleiter hat uneingeschränkten Zugang zu Risikoinformationen aus dem RM

Need-to-Know-Prinzip wird sichergestellt, da der Risikobericht streng vertrauliche Informationen enthält.

Kritische Verwendung / ggf. Hinterfragung der zu verwendenden Informationen

Inhalt/Vorgehen

- Einholung der Dokumente: Risiko-Inventar, Risikomanagement-Berichte, Ad-hoc Meldungen, etc.
- Sichtung der Risiken und Abgleich, ob diese lückenlos existierenden Risikoobjekte des Audit Universe zugeordnet werden können. Falls nicht, entsprechende Risikoobjekte im AU ergänzen
- Informationen aus dem RM systematisch in die Risikobewertung der einzelnen Risikoobjekte im Audit Universe einbeziehen

Alternativen

- regelmäßige Standardprüfung des Jahres x, Prüfung RM-Umsetzung in Jahr x+1, Prüfung RM in ausgewähltem Unternehmens-bereich in Jahr x+2 etc.

Empfehlungen

- neu gemeldete Risiken bzw. betroffene Prüffelder ggf. im nächsten Zyklus als Prüfung einplanen
- umgekehrt ggf. nicht gemeldete Risiken bzw. entsprechende Unternehmensbereiche zu prüfen, um sicherzustellen, dass diese tatsächlich keine Risiken enthalten

IR-Prozess und mögliche Aktionsbereiche

	Übergreifend	Planung	Vorbereitung	Durchführung	Bericht	Follow-up
Leicht			17 Detail-Sichtung des Risiko-inventars hinsichtlich Prüfungs-auftrag			
Mittel			18 Prüfungs-spezifisches Interview mit verantwort-lichem Risiko-manager im Rahmen des Stakeholder Feedbacks			
Komplex						

Ziele der Phase "Vorbereitung"

- Einholung einer Experten-/Drittmeinung zur Risikobewertung eines Sachverhalts in der Phase der Vorbereitung einer Prüfung.
- Die Risikoeinschätzung der IR soll fundiert und ggf. abgesichert werden, um sachgerecht die Prüfung vorbereiten zu können. Zu diesem Zwecke werden im Rahmen der Informationssammlung zusätzlich analytische Prüfungshandlungen durchgeführt und auf deren Basis Thesen erstellt, die in Prüfungsschwerpunkten und/oder konkreten Prüfungsfragen münden.
- Ausarbeitung des detaillierten Prüfprogramms in Form zu bearbeitender Fragestellungen, zu verwendender Vorgehensweisen und einzubeziehender Personen, Materialien und Vorgehensweisen.

Wie kann der IR-Prozessschritt “Vorbereitung” mit Hilfe des RM verbessert werden?

Detail-Sichtung des Risikoinventars hinsichtlich Prüfungsauftrag

Phasen

Vorbereitung
Bericht

Push/Pull

Wechselseitig
Push IR
✓ **Pull IR**

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Ole Wertenbruch

Motivation

- Ggf. unvollständige Informationen oder Differenzen in der Bewertung bekannter Sachverhalte
- (schnelle) Übersicht über die im Prüffeld enthaltenen, bereits identifizierten Risiken

Begründung

- IPPF 2010 Planning
- IPPF 2100 Nature of Work
- IPPF 2210.A1 Engagement Objectives
- IPPF 2310 Identifying Information

Form

- Dokumenteneinsicht, Risk Register
- ggf. zzgl. Mail/Telefonat/Meeting

Teilnehmer

- Prüfer oder Prüfungsleiter

Häufigkeit

- i.d.R. anlassbezogen, aber möglichst systematisch in jeder Prüfung

Ziel

Abgleich der eigenen (IR) Risikoeinschätzung für einen einzelnen, vorgesehenen Prüfungsbereich mit aktuellen Informationen aus dem RM mit dem Ziel einer vollständigen und aktuellen Risikoeinschätzung => Grundlage für Prüfungsauftragsplanung (Prüfprogramm / Schwerpunkte)

Voraussetzungen

IR hat Zugang zu den relevanten Informationen aus dem RM / eigenständiger und uneingeschränkter Zugriff auf das Risikoinventar

Kurzfristige Terminabstimmung möglich

Inhalt/Vorgehen

- Zugriff auf aktuelles Risk Register, bzw. Zusendung des Dokumentes
- Abgleich mit vorläufiger Einschätzung, ggf. Fragen formulieren oder Abweichung begründen
- Rückschluss Risiko-Ursachen im Inventar auf zugehörige Prozesse und Kontrollen
- Ggf. Ergänzung durch individuelle Abstimmung / Kontaktaufnahme mit zuständigem Risk Manager

Alternativen

- Direktzugriff vs. Anfrage der Dokumente
- Mit/ohne persönliches Gespräch

Empfehlungen

- In Vorbereitung zur jeweiligen Prüfung, kurzfristige Abstimmung mit RM, um ggf. auftretende Detailfragen zu klären
- Übereinstimmende Vorgehensweisen und Bewertungskriterien von IR/RM von Vorteil („gemeinsame Sprache“) erleichtern das Verständnis
- Informeller Austausch mit zuständigem Risikomanager erbringt mitunter wertvolle Zusatzinformationen

Stakeholder Feedback: Prüfungsspezifisches Interview mit verantwortlichem Risikomanager

Phasen

Vorbereitung
Bericht

Push/Pull

Wechselseitig
Push IR
✓ **Pull IR**

Schwierigkeit

Leicht
✔ **Mittel**
Komplex

Kontakt

Inga Fabian

Motivation

- Ggf. fehlende Detailinformationen zu den Risiken und Zusammenhängen im Bereich der aktuellen Prüfung

Begründung

- IPPF 2310: Identifikationen von Informationen
- IPPF 2210.A1 und IPPF 2210.A2 --> Einschätzung der Risiken des zu prüfenden Tätigkeitsbereiches vornehmen

Form

- Ordentliches Meeting zu einem, mit dem RM abgestimmten, Termin
- Dauer: Je nach Prüffeld und vorhandenen Risiken 30-90min

Teilnehmer

- Prüfungsleiter und RM-Zuständiger

Häufigkeit

- anlassbezogen, jedoch regelmäßig in jeder Prüfung

Ziel

Einholung einer Experten-/Drittmeinung zur Risikoeinschätzung des Prüfgebietes

Voraussetzungen

gegenseitiges Verständnis mit RM im Sinne regelmäßiger Beanspruchung durch IR

Inhalt/Vorgehen

- Besprechung des Prüffeldes und Identifikation potenzieller Prüfungsschwerpunkte

Alternativen

- nur in ausgewählten Prüfungen, falls nicht grundsätzlich möglich/sinnvoll

Empfehlungen

- Nach Möglichkeit persönlich treffen
- Es sollte ein Ergebnisprotokoll erstellt werden
- Ergebnisse sollten dann in Prüfungskonzeption und Prüfungsauftrag einfließen.

IR-Prozess und mögliche Aktionsbereiche

	Übergreifend	Planung	Vorbereitung	Durchführung	Bericht	Follow-up
Leicht	Ziele der Phase "Durchführung" • Durchführen des geplanten Prüfprogramms • Evaluierung der definierten Prüfobjekte anhand von Interviews, Dokumentensichtungen oder Stichprobenprüfungen • Schaffung von Transparenz bzgl. des Vorhandenseins von Abweichungen zu dem definierten Sollzustand (u.a. Prozesse, Richtlinien) • Definition von Nichtkonformitäten, Handlungsbedarfen oder Verbesserungen • Identifikation und Klassifikation von Risiken • Erarbeitung und Vorbesprechung von Maßnahmen zur Verbesserung der Risikosteuerung			19 Expertise bei Bewertung von Risiken einholen 20 Ad-hoc Meldung identi-fizierter Risiken durch IR		
Mittel						
Komplex						

Wie kann der IR-Prozessschritt "Durchführung" mit Hilfe des RM verbessert werden?

Expertise bei Bewertung von Risiken einholen

Phasen

Planung
Bericht

Push/Pull

Wechselseitig
Push IR
✓ **Pull IR**

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Karsten Sepetauz

Motivation

- Quantitative oder vergleichende Bewertung von Risiken und potentiellem Schadensausmaß ist eine Herausforderung und erfordert ggf. zusätzliche Bewertungsexpertise
- Fehlen relevanter und aktueller Risikoinformationen über nicht kürzlich geprüfte Bereiche
- (neue) Risiken des konkreten Prüfungsobjekts sollen angemessen eingeschätzt werden

Begründung

- IPPF 2210.A1 und IPPF 2210: Einschätzung der Risiken des zu prüfenden Tätigkeitsbereiches
- IPPF 2100, IPPF IG 2100: Beitrag zur Verbesserung / Proaktive Weitergabe von Insights
- IPPF 2000, IPPF IG 2000: Wertbeitrag für die Organisation (Wege zur Verbesserung der Führungs-, Überwachungs-, Risikomanagement und Kontrollprozesse)

Form

- Telefonat oder Meeting
- Dauer je nach Anlass

Teilnehmer

- Prüfungsleiter (ggf. Leiter IR, je nach Größe der Organisation),
- Ansprechpartner für RM (ggf. Leiter RM, je nach Größe der Organisation)

Häufigkeit

- Anlassbezogene Nutzung

Ziel

Einholung einer Experten-/Drittmeinung zur Risikobewertung eines Sachverhalts

Risikoeinschätzung der IR soll fundiert und ggf. abgesichert werden, um sachgerecht die weitere Prüfung durchführen und angemessene Beurteilungen vornehmen zu können

Voraussetzungen

IR kennt verwendete RM-Tools und sieht Risikobeschreibungen vorab ein

Risikoidentifikation und zugehörige (erste) Bewertungen müssen von den Beteiligten erfolgt sein

Inhalt/Vorgehen

- IR koordiniert kurzfristigen, formlosen telefonischen Austausch mit RM und ggf. dem Revisionskunden
- IR dokumentiert die Erkenntnisse zur fraglichen Risikobewertung in den Arbeitspapieren / Aktennotiz
- in Abhängigkeit des zu bewertenden Sachverhalts anschließend das Prüfungsteam informieren

Alternativen

- ggf. Meeting statt Telefonat
- ggf. First oder Second Line-Experte zur Risikoeinschätzung hinzuziehen

Empfehlungen

- Schneller Austausch i.d.R. wichtiger als Formalität
- Klärung zunächst auf Arbeitsebene statt auf Leitungsebene
- Wo nötig schriftliche Einschätzung / Bestätigung einholen
- Bei deutlich unterschiedlichen Risikobewertungen durch RM und IR: 1. Eskalation in RM wegen unterschiedlichen Bewertungsauffassungen innerhalb der Organisation. 2. Dokumentation durch IR in den Arbeitspapieren und - falls keine Einigkeit erzielt werden kann - im Bericht. 3. IR hält innerhalb der Prüfung an ihrer objektiven Einschätzung fest

Ad-hoc Meldung identifizierter Risiken durch IR

Phasen

Durchführung

Übergreifend

Push/Pull

Wechselseitig

✓ **Push IR**

Pull IR

Motivation

- "Berufliche Offenlegungspflicht"
- "Gefahr im Verzug - dringender Handlungsbedarf wird ersichtlich"

Begründung

- IPPF 2060 (Berichterstattung an die Geschäftsführung; „… wesentliche Risikopotentiale“)

Schwierigkeit

✔ **Leicht**

Mittel

Komplex

Kontakt

Markus Silber

Form

- Meldung/Dokument/Mail - idealerweise schriftlich - ggf. Telefonat vorab

Teilnehmer

- Verteiler: Leiter IR, RM und Fachabteilung
- Compliance, evtl. Vorstand (bei hohem Schweregrad und Gefahr im Verzug)

Häufigkeit

- Anlassbezogen, bei aufgetretenen, neu identifizierten Risiken

Ziel

Information der involvierten Bereiche / Stellen über noch nicht erkannte Risiken

Anstoß der ordentlichen Erfassung und ggf. schneller Reaktion

Abstimmung der weiteren Schritte

Voraussetzungen

Relevanter Erwartungswert und hinreichende Feststellung des identifizierten Risikos

Inhalt/Vorgehen

- Sachliche Darstellung des aktuellen Sachverhalts mit vorläufiger Risikobeurteilung (Auswirkungen + Eintrittswahrscheinlichkeit)
- Ansprache mit Fachabteilung im Laufe der Prüfung, Auftrag zur Meldung an Risikomanagement
- Je nach Wertgrenze Vorab-Meldung des neu identifizierten Risikos an Risikomanagement
- Fachabteilung und Risikomanagement übernehmen die ordentliche Erfassung

Alternativen

- Kurzfristiger, formloser Austausch noch bei Anfangsverdacht
- Schriftliche Mitteilung an Risikomanagement
- Zusätzliche Ad-Hoc Meldung an den Vorstand, bei Wesentlichkeit und wenn Gefahr im Verzug ist

Empfehlungen

- Ad-hoc Meldung auf einen puren Anfangsverdacht hin sollte nicht erfolgen
- Ad-hoc Meldungen sollten immer in schriftlicher Art und Weise erfolgen
- Erstellung eines Templates mit den wesentlichen Eckdaten, so dass eine gute Übersicht und Kontinuität gewährleistet ist
- Zumindest: Sachverhalt, Wesentlichkeit, Dringlichkeit, Prozess/Abteilung, Erfasser, Datum

IR-Prozess und mögliche Aktionsbereiche

	Übergreifend	Planung	Vorbereitung	Durchführung	Bericht	Follow-up
Leicht						
Mittel						
Komplex						

Ziele der Phase "Bericht"

- Zusammenfassung der Prüfungs-Ergebnisse für die entsprechenden Stakeholder
- Abstimmung des Auditergebnisses mit dem Auditee
- Aufzeigen der Abweichungen zu dem definierten Sollzustand (u.a. Prozesse, Richtlinien) und der identifizierten Risiken
- Dokumentation von Maßnahmen, um die Risiken zu mitigieren
- Grundlage für die Berichterstattung an die entsprechenden Management-Gremien des Unternehmens
- Berichtsversand an definierten Verteiler

21

Verteilung / Berichts-verteiler Revisions-berichte

Wie kann der IR-Prozessschritt “Bericht” mit Hilfe des RM verbessert werden?

Verteilung / Berichtsverteiler Revisionsberichte

Phasen

Bericht
Übergreifend

Push/Pull

Wechselseitig
✓ **Push IR**
Pull IR

Motivation

- Vermeidung fehlender Information betroffener Stakeholder über aktuellen Zustand, neue Informationen und notwendige Maßnahmen

Begründung

- IPPF 2400 Berichterstattung
- IPPF 2440 Verbreitung der Ergebnisse

Schwierigkeit

Leicht
✔ **Mittel**
Komplex

Kontakt

Inga Fabian

Form

- Mail mit definiertem Berichtsverteiler oder anderes Medium (Informationsraum mit definierten Zugriffsrechten)

Teilnehmer

- je nach Definition des IR-Berichts-wesens, z.B. Geschäftsleitung, Leitung geprüfter Bereich, Leitung RM

Häufigkeit

- Regelmäßig, nach Abschluss jeder Revisionsprüfung

Ziel

Information des geprüften Bereiches über Findings

Information der Geschäftsleitung und Leitung RM über Findings und Risikopotentiale im entsprechenden Prüffeld

Revisionsfeststellungen können durch das Risikomanagement ganzheitlich bewertet und ggf. in das Risikoinventar aufgenommen werden

Voraussetzungen

Anforderungen: Berichtsverteiler sollte nachdem "Need-to-Know"-Prinzip vergeben werden, d.h. Endergebnisse an diejenigen Beteiligten kommunizieren, die sicherstellen können, dass die Ergebnisse angemessene Beachtung unter Einhaltung der gebotenen Vertraulichkeit finden

Inhalt/Vorgehen

- Versand des Revisonsberichtes mit Fristsetzung zu möglichen Anmerkungen o.ä. per Mail
- Bericht als Anhang beifügen

Alternativen

- Teilbericht zu Feststellungen/Risiken, die aus Sicht der Revision relevant fürs RM sind (s. hierzu auch Ad-Hoc Meldung zu identifizierten Risiken)

Empfehlungen

- gemeinsame Regelung treffen, nach der über cc entschieden wird

IR-Prozess und mögliche Aktionsbereiche

Übergreifend	Planung	Vorbereitung	Durchführung	Bericht	Follow-up

Leicht

Mittel

Komplex

Ziele der Phase "Follow-up"

- Schaffung von Transparenz über den Stand von umgesetzten und nicht umgesetzten Maßnahmen
- Aufzeigen der Risiken, die durch die Nicht-Umsetzung von Maßnahmen verbleiben und wie die Verantwortlichen damit umgehen
- Überwachung der Umsetzung von abgestimmten und festgelegten Maßnahmen
- Sicherstellung, dass Maßnahmen effektiv und nachvollziehbar umgesetzt wurden und damit das mit der Feststellung verbundene Risiko wirksam gesteuert bzw. reduziert wurde. Die verantwortliche Geschäftsleitung hat im Zweifel das verbleibende Risiko bei Nicht-Umsetzung zu übernehmen.

22 Information über aktuellen Umsetzungs-grad der Maßnahmen

12 Integrierter GRC-Bericht

Wie kann der IR-Prozessschritt “Follow-up” mit Hilfe des RM verbessert werden?

Integrierter GRC-Bericht

Phasen

Bericht

Bericht

Push/Pull

Wechselseitig
✓ **Push RM**
Pull RM

Schwierigkeit

Leicht
✔ **Mittel**
Komplex

Kontakt

Sebastian Bleich/
Peggy Lilge/
Gabriele Wieczorek

Motivation

- Steigerung der Qualität der Risikoberichterstattung im Sinne eines integrierten Governance / Combined Assurance Ansatzes

Begründung

- Interne Vorgabe zur Berichterstattung und DIIR Nr. 1
- IPPF 2050 „Koordination und Vertrauen“
- IPPF 2060 „Berichterstattung an leitende Führungskräfte“
- Combined Assurance Ansatz

Form

- Auftakt-Meeting vor Dokumenterstellung
- Dokument

Teilnehmer

- Governance-Funktionen des Unternehmens, z.B. Revision, Risikomanagement, Compliance, IKS, Legal ggf. Leitung der Funktion

Häufigkeit

- Regelmäßig
- Definition der Frequenz durch Vorstand bzw. Aufsichtsrat

Ziel

Integrierte Darstellung der Gesamtrisikosituation auf Basis der Assurance-Aktivitäten der 2. und 3. Verteidigungslinien im Unternehmen.

Vermeiden von Information-Overflow aufgrund multipler, uneinheitlicher und widersprüchlicher Berichterstattung

Integrierter GRC-Bericht als "Single Source of Truth"

Voraussetzungen

Auftrag vom Vorstand zur Erstellung eines integrierten GRC-Berichts

Definition der Governance-Funktionen, die zum GRC-Bericht beitragen

Einigung auf gemeinsame Darstellungsform für GRC-Bericht

Inhalt/Vorgehen

- Ausarbeitung Berichtsvorlage (mit jährlicher Evaluierung und Anpassung an interne und externe Anforderung)
- Auftakt-Meeting zur Vorstellung und Abstimmung der folgenden Inhalte
- Individuelle Arbeit am Dokument mit den abgestimmten Inhalten
- Abstimmung des vorfinalen Dokuments, ggf. mit einem Berichtsempfänger
- Befüllen des Berichts z. B. mit Statistiken, durchgeführten Assurance-Aktivitäten im Berichtszeitraum, wesentliche identifizierte Risiken gemäß einheitlicher Methodologie

Alternativen

- Jeder füllt den Bericht für sich aus und stimmt die Berichtsteile ab.

Empfehlungen

- Austausch zwischen den Governance-Funktionen hinsichtlich des jeweiligen Prüfungsscope, Risikobewertungsmethode, Risikodefinition/-Sprache und Form der individuellen Berichterstattung z.B. im Governance-Workshop
- Erarbeitung von Schnittmengen zwischen den Governance-Funktionen und Vereinheitlichung von Risikobewertungsmethoden und Risikosprache oder entsprechende „Übersetzung“ unterschiedlicher Ansätze auf einen gemeinsamen Nenner, z.B. im Governance-Workshop.
- Softwaregestützte Berichterstellung
- Reifegrad des GRC-Berichts hängt vom Reifegrad des integrierten GRC-Ansatzes sowie einer GRC-Strategie ab
- Abgleich mit Perspektive der Wirtschaftsprüfer im Hinblick auf die Erfüllung von Prüfungsvorgaben (inhaltliche Themen)

Information über aktuellen Umsetzungsgrad der Maßnahmen

Phasen

Follow-up
Steuerung

Push/Pull

Wechselseitig
✓ **Push IR**
Pull IR

Motivation

- Herausforderung: Risikoinventar ist ggf. nicht Up-To-Date

Begründung

- IPPF 2500 Monitoring Progress: Der Leiter der Internen Revision muss ein System zur Überwachung der Erledigung der Feststellungen in den dem Management übergebenden Revisionsberichten entwickeln und pflegen

Schwierigkeit

✔ **Leicht**
Mittel
Komplex

Kontakt

Bernhard Geiger

Form

- Meldung/Telefonat/Meeting/ Dokument/
- situations- und gegenstandsbezo-gene Auswahl der Form, abhängig von Dringlichkeit, Komplexität und Bedeutung des Sachverhalts

Teilnehmer

- Führungsebene, d.h. Leiter Revision und Leiter RM (und/oder an verantwortliche Empfangsstelle im RM)

Häufigkeit

- i.d.R. anlassbezogen

Ziel

unterjährige anlassbezogene aktualisierte Risikoinformationen an das Risikomanagement zur ggf. Reaktion über Risikomaßnahmen

Voraussetzungen

zeitnahe Reaktion (Kommunikation bei Fristüberschreitung zeigt Risikosensibilität, Verbindlichkeit und Nachdruck bzgl. einmal vereinbarter Maßnahmen mit den Fachbereichen) => Akzeptanz und Respekt bzgl. der Position der IR bei den Fachbereichen

Inhalt/Vorgehen

- aktives Zugehen auf RM ggf. unterstützt durch geeignete Dokumente (vereinbarte Maßnahmen/Ausschnitt aus Revisionsbericht, Fristen, Lieferungen oder Nicht-Lieferungen der Maßnahmen oder Nachweise)

Alternativen

- a) informelle Berichterstattung an RM
- b) formale standardisierte Berichterstattung an das RM im Rahmen standardisierter, vordefinierter Eskalationsprozesse

Empfehlungen

- Sinnvoll z.B. bei auffälliger Häufung von Fristüberschreitungen bzgl. Umsetzungsvereinbarungen von Maßnahmen aus Revisionsberichten oder insgesamt gehäufte Feststellungen in der Qualität der rückgemeldeten Erledigt-Meldungen in bestimmten Fachbereichen
- beide Varianten je nach Situation gezielt nutzen: sowohl formales standardisiertes Vorgehen im Rahmen von Eskalationsprozesse als auch (zusätzlich) ergänzender informeller Austausch über die Sachverhalte mit RM (=> Tonspur)

Weitere Informationen

Zum Arbeitskreis Interne Revision und Risikomanagement:

Der Arbeitskreis wird gemeinsam aus dem Deutschen Institut für Interne Revision e.V. und der RMA Risk Management & Rating Association e.V., der unabhängigen Interessenvertretung für die Themen Risikomanagement und Rating im deutschsprachigen Raum, gebildet. Daher setzt er sich aus Revisoren und Risikomanagern zusammen.

Der Arbeitskreis Interne Revision und Risikomanagement verantwortet den DIIR Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision. Im Jahr 2021 traten die beiden Gesetze StaRUG und FISG in Kraft, die Auswirkungen auf die Anforderungen an das Risikomanagementsystem in Unternehmen haben. Beide Initiativen wurden daher in den Standard eingearbeitet. Der Standard berücksichtigt als erster Prüfungsstandard die genannten Gesetze.

Neben dem Standard wurde ein zugehöriger Prüfungsleitfaden und eine Checkliste zur Prüfung des Risikomanagements inklusive quantitativer Auswertung entwickelt und fortlaufend gepflegt. Auch diese Erzeugnisse des Arbeitskreises sind für die Allgemeinheit frei verfügbar.

Im Jahre 2019 hat der Arbeitskreis ein Positionspapier mit Empfehlungen zum Zusammenwirken von Revision und Risikomanagement veröffentlicht, das im Jahre 2022 überarbeitet und erweitert wurde. Die vorliegende Pattern-Sammlung versteht sich als Anhang bzw. konkrete Umsetzungshilfe zu Empfehlungen aus dem Positionspapier.

Weiterführende Literaturempfehlungen:

- Combined Assurance Studie, DIIR e.V., 2020: Diese Studie gibt einen Überblick über die Anwendung, Umsetzungsgrad, potentielle Vorteile und Hindernisse von integrierten Governance- bzw. Combined Assurance-Ansätzen sowie über die Rolle der Internen Revision bei der Implementierung dieses Konzeptes. Die Ergebnisse basieren auf einer anonymisierten Umfrage unter Internen Revisoren aus 149 deutschen Unternehmen.

- Aus der Schriftenreihe „Risikomanagement – Schriftenreihe der RMA“ (2015). Praxisleitfaden Risikomanagement im Mittelstand. Erich Schmidt Verlag. ISBN 978 3 503 165261

Autoren / Ansprechpartner

Dieser Leitfaden wurde erarbeitet vom Arbeitskreis "Interne Revision und Risikomanagement", verbandsübergreifend für das Deutsche Institut für Interne Revision e.V. und die RMA Risk Management & Rating Association e.V.

Die nachfolgend genannten Autoren stehen für Rückfragen und Ihre weiterführenden Gedanken zu den beschriebenen Themen und insbesondere zu den jeweils zugeordneten Aktionskarten zum Austausch bereit.

Interne Revision

Sebastian Bleich

Inga Fabian

Klaus Frech

Bernhard Geiger

Martin Gutzmer

Karsten Sepetauz

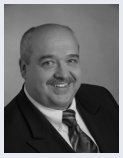
Markus Silber

Ole Wertenbruch

Risikomanagement

Peggy Lilge

Gabriele Wieczorek



Michael Hilser

Peter Rumpf

Stefanie Klein

Lars Düser

Veröffentlichung am 19.10.2022 auf https://www.diir.de/arbeitskreise/interne-revision-und-risikomanagement/

Zu den Verbänden

Über das DIIR - Deutsches Institut für Interne Revision e.V.: Das DIIR ist ein gemeinnütziges Institut zur Förderung und Weiterentwicklung der Internen Revision in Deutschland. Es wurde 1958 gegründet und hat mittlerweile über 3.000 Mitglieder aus allen Bereichen der Wirtschaft, Wissenschaft und Verwaltung. Das DIIR unterstützt seit mehr als 60 Jahren die für Prüfungs- und Beratungsaufgaben zuständigen Fach- und Führungskräfte in ihrer praktischen Arbeit. Fachkundige Persönlichkeiten aus Praxis und Wissenschaft tragen durch ihr vielfältiges Engagement zur Aufgabenerfüllung des DIIR bei.
https://www.diir.de

Über die RMA - Risk Management & Rating Association e.V.: Die RMA Risk Management & Rating Association e.V. ist die unabhängige Interessenvertretung für die Themen Risikomanagement und Rating im deutschsprachigen Raum. Hervorgegangen aus der Risk Management Association e. V. (RMA) und dem Bundesverband der Ratinganalysten e.V. (BdRA) ist der Verband Kompetenzpartner, Impulsgeber und erster Ansprechpartner für Informationen, den unternehmensübergreifenden Dialog sowie die Weiterentwicklung des Risikomanagements und Ratings.
https://rma-ev.org/