Praxisleitfaden Corporate Governance

Hansen / Melchior / Gerke

2022
ISBN 978-3-406-77566-6
C.H.BECK

wertet werden, ob der Aktionsplan den notwendigen Effekt hatte und das Risiko reduziert werden konnte. Dabei muss auch erneut das Umfeld angeschaut und bewertet werden. Sollte der Plan den gewünschten Effekt gehabt haben, wird das Risiko mit dem Zielwert bewertet und auf akzeptiert gesetzt. Sollten sich andere Faktoren ergeben haben (zB eine Verschlechterung des externen Umfelds), muss unter Umständen ein weiterer Aktionsplan angelegt werden und das Risiko bleibt weiterhin offen und kann nicht akzeptiert werden.

Die Risikokoordinatoren sind dazu aufgefordert, mind. zum Ende eines jeden Quartals den Status der Aktionspläne und Risiken in dem zentralen IT-Tool entsprechend zu aktualisieren und zu pflegen. Somit ist eine zentrale und aktuelle Übersicht vom Status aller Risiken gewährleistet. 69

Mögliche Nachweise zur Schließung eines Aktionsplans 70

- Erstellung einer neuen Richtlinie oder eines Leitfadens
  - ❑ Genehmigtes Dokument
  - ❑ Offizielle E-Mail-Kommunikation
  - ❑ Link zum Webinar zur Einführung der Richtlinie
- Einführung einer neuen Kontrolle
  - ❑ Dokumentation der eingeführten neuen internen Kontrolle (Richtlinie, etc.)
  - ❑ Ergebnis einer Stichprobe zur Überprüfung des Vorhandenseins der neuen internen Kontrolle
- Einführung einer neuen Schulung
  - ❑ In der Schulung verwendetes Präsentationsmaterial
  - ❑ Link zur Schulungsaufzeichnung/e-Training
  - ❑ Zusammenfassender Bericht über die Teilnahme an der Schulung/Abschlussquote
- Erstellen einer neuen Rolle/eines neuen Teams
  - ❑ Organisatorische Ankündigung
  - ❑ Organigramm
  - ❑ Charta für Governance und Prioritäten
- Abschluss eines Projekts/Programms
  - ❑ Präsentation der Ergebnisse für das Management (einschließlich Sitzungsprotokoll)
  - ❑ Offizielle Bekanntgabe des erfolgreichen Abschlusses des Projekts/Programms

D. IT-System im Risikomanagement

Jede Einheit, die einen Risiko Workshop durchführt, ist dazu verpflichtet, ihre Ergebnisse in einer zentralen IT-Plattform zu hinterlegen und konstant aktuell zu halten. Die Dokumentation im IT-System erfolgt nicht in Landessprache, sondern einheitlich in Englisch, um globale Auswertungen und Vergleiche zu ermöglichen. Mindestens einmal im Quartal müssen die Risiken und Aktionspläne überprüft werden, um einen aktuellen Status zu gewährleisten. Novartis nutzt eine zentrale IT-Plattform, auf der die Risikomanagement-Software gehostet wird. Das IT-Tool unterstützt den Risikomanagementprozess vollständig. Es werden nicht nur die Risiken und damit verbundenen Daten und Aktionspläne erfasst, sondern auch automatische Erinnerungen verschickt und personalisierte Berichte erstellt. 71

72

Category	Level	When	To Whom	Copy To
Notification	Risk	A new risk is added to the tool	Risk Owner & Risk Co-Owner(s)	Risk Coordinator
Notification	Action Plan	A new Action Plan is added to the tool	Action Plan Owner & Team Members	Risk Coordinator
Reminder	Risk	Periodic risk review reminders for risks with treatment strategy Reduce, Pursue or Share: - End of every quarter (31 Mar, 30 Jun, 30 Sep and 31 Dec)	Risk Owner & Risk Co-Owner(s)	Risk Coordinator
Reminder	Risk	Periodic risk review reminders for risks with treatment strategy Accept or Avoid: Countries: Once in a year (31 Mar) Div/BU/OU/Functions: Once in a year (30 Jun)	Risk Owner & Risk Co-Owner(s)	Risk Coordinator
Reminder	Action Plan	2 weeks before the due date	Action Plan Owner & Team Members	Risk Coordinator
Reminder	Action Plan	2 days before the due date	Action Plan Owner & Team Members	Risk Coordinator

Abb. 19: Automatische Erinnerungen

73 Das IT-Tool bildet alle Hierarchien im Unternehmen ab und ist die „single source of truth" für alle Risiken und deren Aktionspläne. Dies ist wichtig, um keine Schattenberichterstattung von Risiken zuzulassen und ermöglicht so, dem Globalen Enterprise Risk Management Team einen konstanten Überblick über die Risiken, aber auch über den Status der Maßnahmen und deren Abarbeitung zu haben. Das zentrale IT-System wurde 2020 bei Novartis etabliert, da es bereits für andere Services im Unternehmen genutzt wurde und daher relativ einfach und schnell implementiert werden konnte.

74 **Praxistipp – IT-System im Risikomanagement**

- Es gibt eine schier endlose Zahl von Anbietern bzgl. IT-Systemen im Risikomanagement, wobei alle ihre Stärken und Schwächen haben. Eine Prüfung, was bereits im Unternehmen verwendet wird, führt meist zu interessanten Erkenntnissen und kann den Auswahlprozess beschleunigen.
- Es empfiehlt sich, einen Anforderungskatalog mit wichtigen Funktionen vorab zu erstellen und dann mögliche Systeme mit Ihren Standardfunktionen dagegen zu ver-

gleichen. Eine Standardsoftware hat Vorteile zB in Bezug auf go-live Schnelligkeit, Bug-Fixes, Performance und ist einer an den Kunden angepassten Lösung meist vorzuziehen. Gänzlich ohne kleinere Anpassungen ist eine Implementierung aber auch meist nicht möglich.
- Ein IT-System im Risikomanagement sollte auf jeden Fall die Möglichkeit der Skalierung bieten. Alle Risiken und Aktionspläne aus dem Unternehmen, egal ob aus Projekten, von Funktionen, Länder, Divisionen oder gänzlich anderer Bereiche, müssen in dem System erfasst werden können. Nur so kann ein ganzheitliches Enterprise Risk Management auf allen Ebenen sichergestellt werden.
- Neben der Skalierung muss ein IT-System auch die verschiedenen Rollen im Prozess mit unterschiedlichen Rollenprofilen abdecken können. Die Rollenprofile können sich unterscheiden im Zugriff auf die Risiken zB beschränkt auf ein Land, beschränkt auf die divisionalen Risiken weltweit, etc. oder bei den Schreib- und Leserechten.
- Es kann unter Umständen sinnvoll sein, das Enterprise Risk Management IT-System zu erweitern und ebenfalls als „Vorfall" (Incident) Management System zu verwenden. Vorfälle können in gewissen Bereichen eine enge Beziehung zu Risiken haben, gerade im operativen Umfeld. Die Komplexität für das Unternehmen darf hierbei allerdings nicht unterschätzt werden und bedarf einer genauen Voranalyse.[9] Es sollte auch nicht als erster Schritt auf der Agenda stehen.

Ein solches System ist für einen ganzheitlichen Risikoansatz unabdingbar. Wichtig ist es, die verschiedenen Nutzer solch einer Plattform frühzeitig zu identifizieren, ausreichend zu schulen und auf ihre Verantwortlichkeit hinzuweisen. Ansonsten kann es zu vielen Fehlmeldungen oder Frust in der Organisation kommen. Des Weiteren ist es wichtig die Qualität der Einträge sicherzustellen, da Zusammenfassungen und Ableitungen für die Konzernrisiken auf Basis der Daten im IT-Tool getroffen werden. 75

Praxistipp – Datenqualität im Risikomanagement 76

- Bei Eingabe der finalen Risiken und Aktionspläne von den Risiko Workshops sollte das Globale Enterprise Risk Management Team kontaktiert werden, um die Qualität und Verständlichkeit der geplanten Einträge vorab zu prüfen. Generell sollte ein unabhängiger Dritter keine Mühe haben, die erfassten Risiken und Aktionspläne zu verstehen.
- Das Globale Enterprise Risk Management Team sollte in regelmässigen Abständen (zB jedes Quartal) die Datenqualität stichpunktartig kontrollieren, da die Daten kontinuierlich geändert werden, um die Risiken und Aktionspläne aktuell zu halten.
- Die Nutzer des IT-Systems sollten in regelmäßigen Abständen geschult werden. Hierzu können die Ergebnisse aus den Stichproben anonymisiert werden, um konkrete Beispiele der Nutzergemeinschaft sichtbar zu machen. Auch hat es sich bewährt, gänzlich offene Frage und Antwort Stunden den Nutzern anzubieten (zB einmal pro Woche) um zeitnah Probleme zu besprechen und zu lösen.

[9] Novartis hat sich bis dato gegen die Verbindung vom Vorfall- und Risikomanagement entschlossen.

77

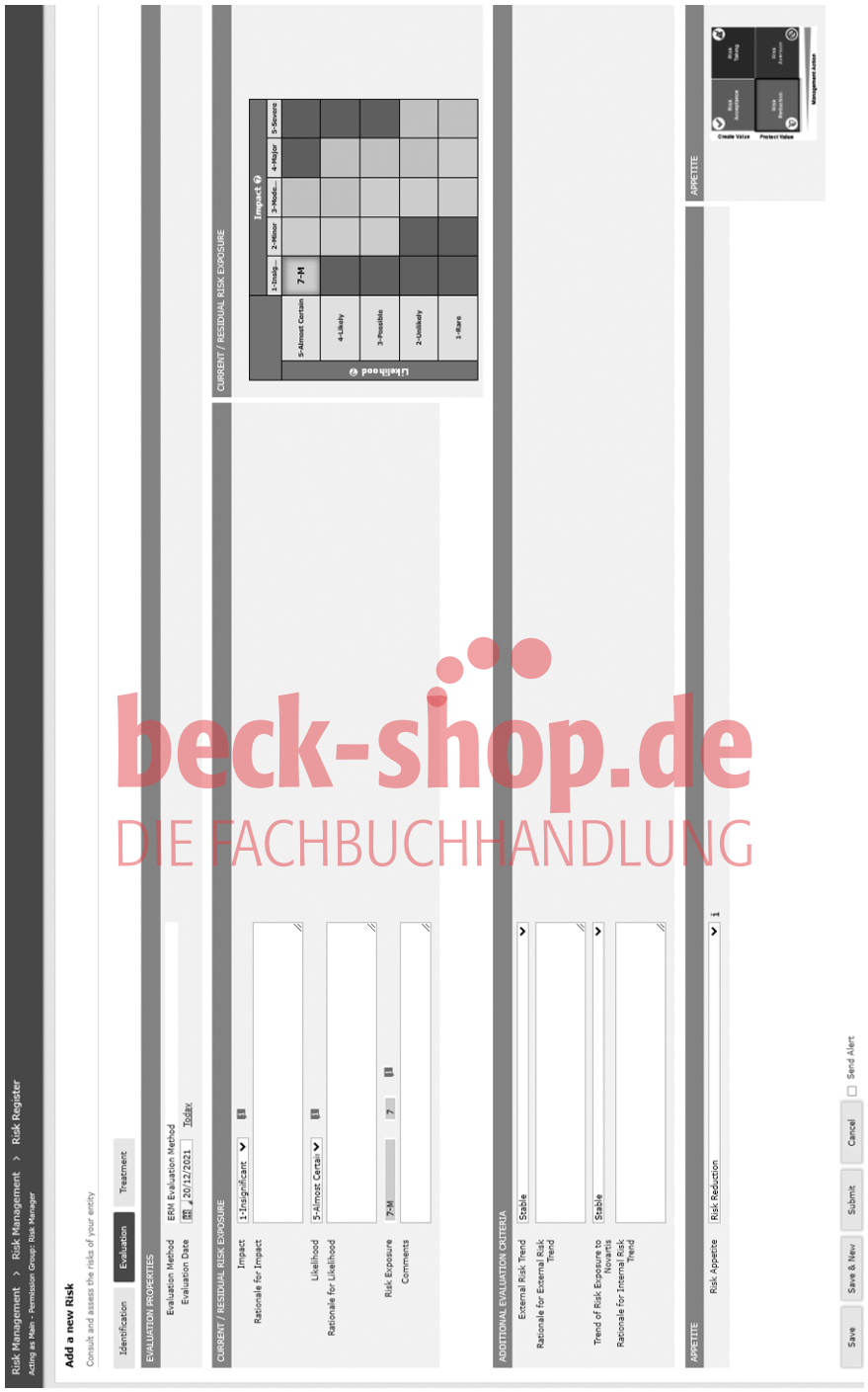

Abb. 20: Screenshot vom zentralen Risikomanagement IT-System

E. Konsolidierung der Ergebnisse auf Unternehmensebene

Im September jeden Jahres findet der jährliche Risiko Workshop mit dem Risk Leadership Team statt, in welchem die Ergebnisse der Risiko Workshops von den Ländern und globalen Einheiten vorgestellt und besprochen werden. Nach dieser Durchsprache findet die Konsolidierung der wichtigsten Risiken für das Unternehmen statt. Das Globale Enterprise Risk Management Team spielt hierbei eine entscheidende Rolle bei der Vorbereitung, Durchführung und Moderation. Der Workshop dauert vier Tage und findet seit 2020, bedingt durch die Covid-19 Pandemie, virtuell statt. 78

Am ersten Tag liegt der Fokus auf den Risiken der Länder. Hierbei werden von den umsatzstärksten Ländern einige Risikokoordinatoren ausgewählt, die ihre Risiken detailliert präsentieren. Aufgrund zeitlicher Beschränkungen muss eine Landesauswahl getroffen werden. Diese verändert sich von Jahr zu Jahr und wird vom globalen Team festgelegt. Hauptaugenmerk liegt auf den fünf wichtigsten Risiken, Veränderungen im Vergleich zum Vorjahr (starker An- oder Abstieg, neue Risiken, Verfall von Risiken), sowie den Aktionsplänen der Risiken. Im Anschluss an die Vorträge besteht die Möglichkeit, in der Gruppe Fragen zu stellen und Details zu diskutieren. Dieser Austausch direkt mit den Ländern ist wichtig und hilft Trends frühzeitig zu erkennen. Im Anschluss an die Einzelpräsentation trägt das Globale Enterprise Risk Management Team die Konsolidierung aller Landesrisiken vor. Diese Auswertung wird mit Hilfe des IT-Systems vorbereitet und erfasst alle Landesrisiken aus dem jeweiligen Jahr. Hierbei geht es darum, konsolidiert die wichtigsten Risiken aus Landesperspektive zu erkennen, die Veränderungen zum Vorjahr zu verstehen und eine Diskussion mit den Teilnehmern anzuregen, was die Ursachen für die Veränderungen sein könnten. 79

Am zweiten Tag ist der Fokus auf die Risiken der globalen Divisionen und Organisationseinheiten gerichtet, wobei hier alle Einheiten präsentieren. Der Fokus liegt ebenfalls auf den fünf wichtigsten Risiken, Veränderungen im Vergleich zum Vorjahr (starker An- oder Abstieg, neue Risiken, Verfall von Risiken), sowie den Aktionsplänen der Risiken. Auch hier wird vom globalen Team eine Konsolidierung vorbereitet und mit den Teilnehmern diskutiert. 80

Am dritten Tag präsentieren die globalen Funktionen wie zB Finanz, Steuer, Qualität, Datenschutz oder Informationssicherheit ihre funktionsspezifischen Risiken. Hierbei geht es darum, global relevante Risiken zu identifizieren, die einen signifikanten Einfluss auf das gesamte Unternehmen haben können. Da diese Risiken Einzelfunktionen abdecken und es normalerweise keine größeren Schnittmengen gibt, findet hier keine Konsolidierung vorab durch das globale Team statt. 81

Am vierten Tag erfolgt die Konsolidierung der Risiken auf oberster Unternehmensebene. Der Workshop beginnt mit einer Präsentation der Strategie Abteilung, um die strategische Ausrichtung des Unternehmens mit allen Teilnehmern zu reflektieren. Anschließend stellt die Audit Abteilung eine Zusammenfassung der wichtigsten Audit-Trends aus dem laufenden Jahr vor. Daneben wird ein Vortrag zu Wettbewerbern und deren veröffentlichten Risiken, sowie generellen externen Risiko Trends aus Quellen von den Big4 (PwC, KPMG, E&Y, Deloitte), Banken und Versicherungen gehalten. Darauf folgt eine offene Diskussion, in welcher die finale Risiko Matrix für das Unternehmen erstellt wird. Ein erster Entwurf der Risiko Matrix wird vom Globalen Enterprise Risk Management Team anhand der Ergebnisse der vorherigen Tage vorbereitet. Die Risiken werden entsprechend der Methodik in strategische, operative oder sich entwickelnde (emerging) Risiken kategorisiert. Auch die globalen Aktuellen Themen (Awareness Topics) werden in der Runde besprochen und finalisiert. 82

Der abschließende Entwurf der Risiko Matrix für das Unternehmen wird nun weiter intern mit Mitgliedern der Geschäftsleitung vorbesprochen und im Anschluss in einer Geschäftsleitungssitzung offiziell verabschiedet. 83

84

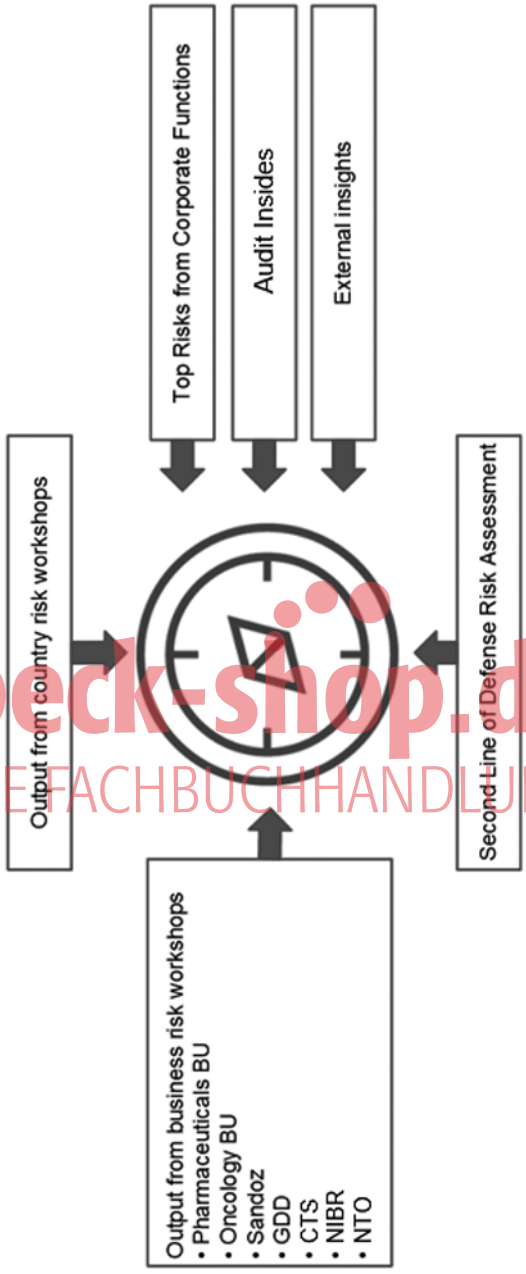

Abb. 21: Informationen für den Risiko Workshop

F. Berichterstattung

Nach der offiziellen Verabschiedung der Risiko Matrix für das Unternehmen durch die Geschäftsleitung werden zu den einzelnen Risiken Details mit den Risikoverantwortlichen erstellt. Dies beinhaltet eine Beschreibung des Risikos, den aktuellen Status, Fortschritt im vergangenen Jahr (falls über das Risiko bereits berichtet wurde) und Aktionspläne für die Zukunft mit Verantwortlichen und Fristen. Die einzelnen Risiken werden dann in dem internen „Novartis Annual Risk Report" (Risiko Bericht) zusammengefasst, wobei neben den Risiken auch die Weiterentwicklung des Risikoprozesses beschrieben wird. Der Bericht wird dem Risikoausschuss des Verwaltungsrats am Ende eines jeden Jahres zur Verfügung gestellt und präsentiert. Der Bericht bildet ebenfalls die Grundlage für das sog. Form 20-F[10], welches Novartis aufgrund seiner Tätigkeiten in den Vereinigten Staaten veröffentlicht. Des Weiteren werden Auszüge der wichtigsten Risiken im Novartis In Society Report[11] und auf der externen Internet Seite veröffentlicht[12]. 85

[10] https://www.novartis.com/sites/novartis_com/files/novartis-20-f-2020.pdf Seite 11 ff
[11] https://www.novartis.com/sites/novartis_com/files/novartis-in-society-report-2020.pdf Seite 21 ff
[12] https://www.novartis.com/sites/novartis_com/files/novartis-enterprise-risk-management.pdf