

# **Praxisleitfaden Corporate Governance: Zusammenspiel von Risikoidentifizierung, Richtlinienmanagement und Internem Kontrollsystem**

Hansen / Melchior / Gerke

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

schnell und portofrei erhältlich bei  
[beck-shop.de](https://www.beck-shop.de)

Die Online-Fachbuchhandlung [beck-shop.de](http://beck-shop.de) steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.

[beck-shop.de](http://beck-shop.de) hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird [beck-shop.de](http://beck-shop.de) für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Hansen/Melchior/Gerke

Praxisleitfaden Corporate Governance:  
Zusammenspiel von Risikoidentifizierung,  
Richtlinienmanagement und Internem Kontrollsystem



**beck-shop.de**  
DIE FACHBUCHHANDLUNG

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

# Praxisleitfaden Corporate Governance: Zusammenspiel von Risikoidentifizierung, Richtlinienmanagement und Internem Kontrollsystem

Ein Praxisleitfaden am Beispiel eines  
multinationalen Konzerns

von  
**beck-shop.de**  
von  
**Jan Hansen**  
Program Lead: Transformation for Growth, Novartis AG  
**Susanne Melchior**  
DIE FACHBUCHHANDLUNG

Head Risk and Internal Control, Novartis AG

und

**Ulrike Gerke**

Head Enterprise Policy Management, Novartis AG

2022



Zitiervorschlag:  
HMG Praxisleitfaden Corporate Governance § ... Rn. ...

  
**beck-shop.de**  
DIE FACHBUCHHANDLUNG

**[www.beck.de](http://www.beck.de)**

ISBN 978 3 406 77566 6

©2022 Verlag C.H. Beck oHG

Wilhelmstraße 9, 80801 München

Druck und Bindung: Druckerei C.H. Beck Nördlingen  
(Adresse wie Verlag)

Satz: 3w+p GmbH, Rimpfing

Umschlaggestaltung: Martina Busch, Grafikdesign, Homburg Saar



[chbeck.de/nachhaltig](http://chbeck.de/nachhaltig)

Gedruckt auf säurefreiem, alterungsbeständigem Papier  
(hergestellt aus chlorfrei gebleichtem Zellstoff)

## Vorwort

Über das Zusammenspiel von Risikoidentifizierung, Richtlinienmanagement und Internem Kontrollsystem ist – insbes. aus Sicht der Berater – schon einiges geschrieben worden, meistens unter dem Stichwort „Governance, Risk and Compliance (GRC)“. Schwerer zu finden sind allerdings Veröffentlichungen zur praktischen Implementierung eines solchen Systems. Dies liegt zum einen daran, dass es in vielen Unternehmen an den entsprechenden Organisationsstrukturen für die erfolgreiche Zusammenführung der verschiedenen Elemente eines GRC fehlt. Zu oft noch sind das Management von Risiken, Unternehmensrichtlinien und internen Kontrollen in verschiedenen Einheiten verortet und insbes. nicht mit dem Compliance Programm des Unternehmens verbunden. Zum anderen wird oft auf die Verschiedenheit der Unternehmensstrukturen und Risikoprofile verwiesen, die allgemein gültige Aussagen zu einem effektiven GRC System erschweren. Letzterer Einwand ist nicht einfach von der Hand zu weisen und so soll auch der hier von einem Team leitender Mitarbeit\*innen der Novartis Ethics, Risk und Compliance Funktion vorgelegte Praxisleitfaden nicht als „copy-paste“ Aufforderung verstanden werden. Vielmehr geht es darum, unsere bisherigen Erfahrungen bei der Verbindung von Risikoidentifizierung, Richtlinienmanagement und internem Kontrollsystem als ein Beispiel für einen umfassenden Corporate Governance Rahmen zu erläutern und damit einen praxisorientierten Beitrag zur Diskussion, um die „Assurance“ in Unternehmen zu leisten. Gerade in einer Zeit, in der die Gesellschaft und damit auch die Krisenfestigkeit und Resilienz der Unternehmen durch die weltweite Pandemie und den Krieg in der Ukraine auf den Prüfstand gestellt werden, ist diese Diskussion wichtiger denn je.

Basel, im Januar 2022

*Dr. Klaus Moosmayer*  
Mitglied der Geschäftsleitung und  
Chief Ethics, Risk and Compliance Officer der Novartis AG

beck-shop.de  
DIE FACHBUCHHANDLUNG

**beck-shop.de**  
DIE FACHBUCHHANDLUNG



# Inhaltsverzeichnis

Vorwort .....	V
Abkürzungsverzeichnis .....	XI
Abbildungsverzeichnis .....	XIII
Tabellenverzeichnis .....	XV

## § 1 Einleitung & Allgemeines

A. Einleitung .....	1
B. Allgemeines .....	5
I. Governance, Risk & Compliance (GRC) .....	5
II. GRC als strategischer Erfolgsfaktor bei Novartis .....	6
III. Historie .....	6

## § 2 Enterprise Risk Management

A. Enterprise Risk Management – Organisation, Gremien und Aufgaben .....	9
B. Zeitlicher Ablauf im Geschäftsjahr .....	11
C. Enterprise Risk Management Prozess .....	13
I. Rollen im Enterprise Risk Management Prozess .....	13
II. Ablauf eines Risiko Workshops .....	15
III. Vorbereitung des Risiko Workshops .....	17
IV. Durchführung des Risiko Workshops .....	22
V. Risikoanalyse .....	26
VI. Risikobewertung .....	30
VII. Risikobehandlung .....	32
VIII. Überwachung und Überprüfung .....	34
D. IT-System im Risikomanagement .....	39
E. Konsolidierung der Ergebnisse auf Unternehmensebene .....	43
F. Berichterstattung .....	45

## § 3 Enterprise Policy Management

A. Enterprise Policy Management – Organisation .....	47
B. Enterprise Policy Management – Governance und Gremien .....	48
I. Aufsicht und Genehmigung durch die Geschäftsleitung .....	48
II. Policy Board .....	48
C. Inhalt und Erstellung .....	49
I. Richtlinienverantwortliche .....	49
II. Stakeholder .....	49
III. Definitionen und Dokumententypen .....	50
D. Enterprise Policy Management Prozess .....	51
I. Generelle Prozessbeschreibung .....	51
II. Erstellen eines Neuen Dokumentes .....	52
III. Feedback von Stakeholdern und Experten .....	53
IV. Interne Freigabe .....	54
V. Vorbereitung zur Genehmigung .....	54

VI. Genehmigung .....	55
VII. Genehmigungsprozess und Freigabestufen bei Novartis .....	55
VIII. Implementierung, Kommunikation und Training .....	56
1. Datum des Inkrafttretens des Dokuments .....	57
2. Erstellung der zugehörigen Dokumente .....	57
a) Übersetzungen .....	57
b) Anpassungen .....	57
3. Beziehungen zwischen Dokumenten .....	58
4. Veröffentlichung der relevanten Kontrollen im Kontrollregister .....	58
IX. Ablage im Dokumentenmanagement System .....	58
X. Archivierung .....	58
XI. Öffentliche Publikationen .....	58
XII. Kommunikation .....	59
XIII. Training .....	59
XIV. Überprüfung .....	60
XV. Außer Dienst stellen von Policies und Richtlinien .....	60
E. Rollen und Verantwortlichkeiten .....	61
I. Richtlinienverantwortlicher/Dokumenteneigentümer .....	61
II. Fachexperten, Stakeholder .....	62
III. Policy Experte .....	62
IV. EPM Team .....	62
VI. Policy Board .....	63
VII. Geschäftsleitung/Vorstand .....	63
F. EPM Richtlinien und Handbücher .....	63
I. EPM Richtlinie .....	64
II. EPM Handbuch .....	64
III. EPM-Dokumentvorlagen/Templates .....	65
IV. Richtlinien, Handbücher, Templates bei Novartis .....	66
V. Systemunterstützung .....	67
G. Praktisches Beispiel – Das Novartis Policy Management Framework .....	70
H. Das Enterprise Policy Management Projekt .....	71
I. Praxistipp: Einbeziehung von Stakeholdern in das EPM Projekt .....	72
J. EPM im täglichen Geschäftsablauf .....	73
I. Governance und Strategie .....	73
1. Compliance und Monitoring .....	73
2. Kommunikation und Change-Management .....	73
II. Operationeller Betrieb .....	74
1. Erstellung .....	74
2. Genehmigung .....	74
3. Implementierung .....	74
K. Fazit .....	75
<b>§ 4 Internes Kontrollsystem</b>	
A. Historie und Generelles .....	77
I. Projekt „In Control“ .....	77
II. Risikomanagement und interne Kontrollen .....	78
III. Policymanagement und interne Kontrollen .....	81
IV. Projektanstoß für einen ganzheitlichen Ansatz für interne Kontrollen .....	81

B. ONCE (One Novartis Control Environment) .....	81
I. Das ONCE Governance Modell .....	84
II. Das ONCE Meta Prozess Modell .....	91
III. Rollen im ONCE Prozess .....	93
C. Der operative ONCE Prozess .....	95
I. Scoping and Assignment .....	96
II. Das Self-Assessment .....	97
III. Kontrolltesting .....	100
1. Voraussetzungen für die Durchführung von Kontrolltests .....	100
2. Typische Schritte zur Durchführung von Kontrolltests .....	101
3. Größe der Teststichprobe .....	101
4. Qualität der Stichprobe .....	102
5. Testmethoden .....	102
6. Dienstleistungen von Drittanbietern für Prozesse im Anwendungsbereich von ONCE .....	102
IV. Das Acknowledgement .....	103
D. Fortlaufende Steuerung und Überwachung .....	104
E. Behebung von Mängeln und Schwachstellen .....	104
F. Beziehungen Globale Funktion und Control Entities .....	104
G. Limitationen bei der Bestimmung des Control Ratings .....	104
H. Kategorien von Kontrollen .....	106
I. Global Governance Controls (GGC) .....	106
II. Segregation of Duties (SOD) Controls .....	109
III. Access Controls/ Zugriffs- und Zutrittskontrollen .....	109
IV. Management Review Controls (MRC) .....	109
V. Fraud Controls/Kontrollen zur Vermeidung oder Entdeckung von Betrug .....	109
I. Das Control Register .....	110
J. Das Entity Universe .....	113
K. Berichterstattung .....	113
L. Die ONCE Software Lösung .....	114
M. Generelle Limitationen eines Internen Kontrollsystems .....	118

## § 5 Abschließende Bemerkungen

Sachverzeichnis .....	121
-----------------------	-----

**beck-shop.de**  
DIE FACHBUCHHANDLUNG