Rödl & Partner

GEMEINSAM ERFOLGREICH

BOC Group
Design Your Enterprise

KRITISCHE GRC-ERFOLGSFAKTOREN UND IHRE SOFORTIGE UMSETZUNG IN ADOGRC

Webinar, 8. Juli 2025

REFERENTEN

Herzlich Willkommen

ALEXANDER KLEINSASSER
Business Development Manager
BOC Group Schweiz

CHRISTIAN UHRIG
Associate Partner
Rödl & Partner

LARISSA STROEHLEN
ADOGRC Produktmanagement
BOC Group

AGENDA

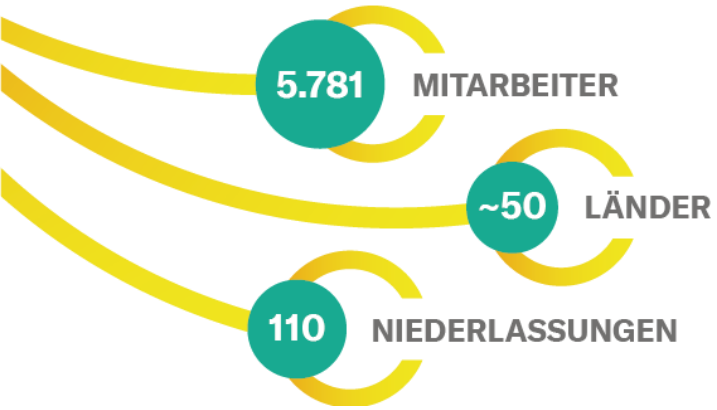
1	Referenten
2	Vorstellung Rödl & Partner & BOC Group
3	GRC-Systeme ❖ Governance ❖ Compliance ❖ Risiko Management
4	Service Offerings

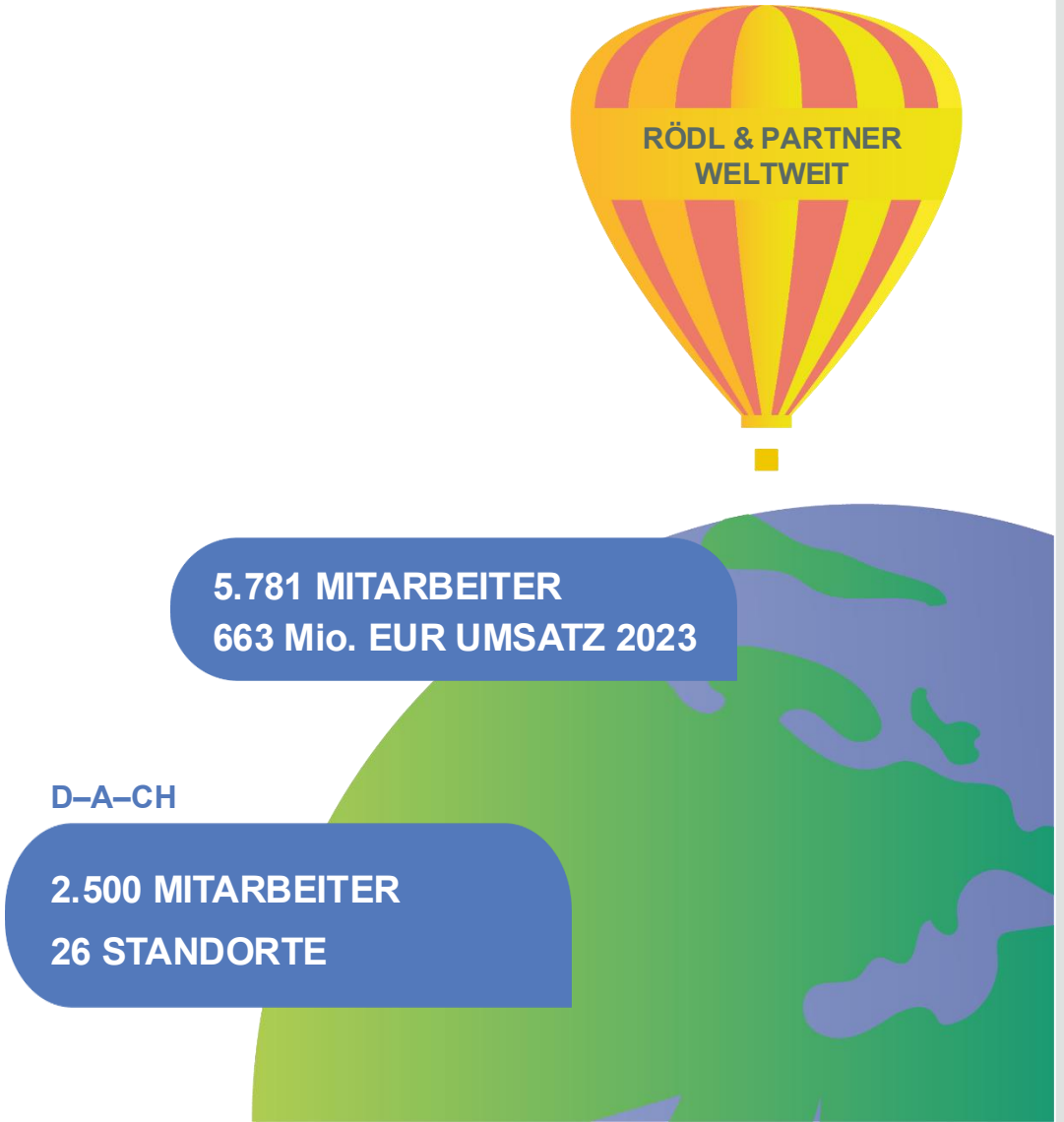
RÖDL & PARTNER

WELTWEIT AUS DEUTSCHLAND HERAUS

Weltweit vor Ort

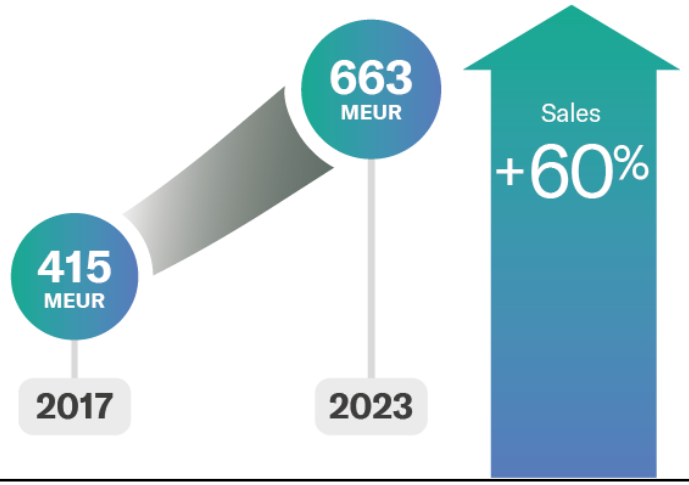
Wir stellen eine lokale Betreuung überall dort sicher, wo deutsche Unternehmen im Ausland vertreten sind. Dabei können wir überwiegend auf **deutschsprachige** Kolleginnen und Kollegen zurückgreifen und Ihnen in jedem Fall Erfahrung in der Betreuung deutscher Unternehmen bieten.





ADVISORY „TAILOR MADE“

Die deutsche Prüfungs- und Beratungsgesellschaft



Rang	Wettbewerber
1	PwC
2	Deloitte
3	KPMG
4	EY
5	Rödl & Partner
6	RSM Ebner Stolz
7	BDO
8	Baker Tilly

Quelle: manager magazin 04/2024;
WGMB Wissenschaftliche Gesellschaft für Management und Beratung mbH, Bonn

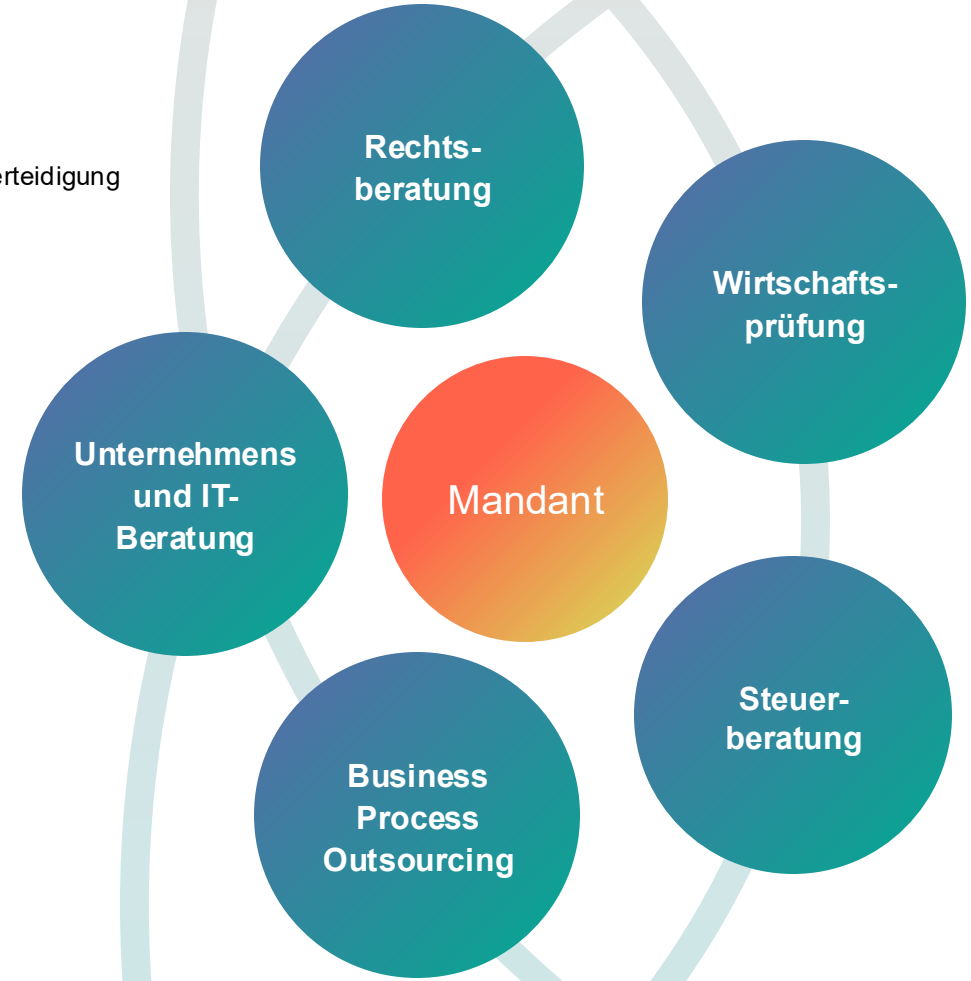
Wir sind die einzige aus Deutschland heraus tätige, international aufgestellte Prüfungs- und Beratungsgesellschaft mit eigenen Niederlassungen im Ausland. Unsere Prozesse sind interdisziplinär, effizient und für deutsche mittelständisch geprägte Weltmarktführer **maßgeschneidert**. Unser Erfolg über die Jahre zeigt, dass dieser Weg von unseren Mandanten geschätzt wird.

UNSERE DIENSTLEISTUNGEN IM ÜBERBLICK

- Gesellschaftsrecht/M&A
- Arbeitsrecht
- Handels- und Wirtschaftsrecht
- Finanz- und Bankrecht
- Nachfolge, Vermögen, Trusts
- Technologie, Daten, IP und Medien
- Compliance, Forensik, Prävention und Verteidigung
- Streitbeilegung, Rechtsstreitigkeiten
- Immobilien, Gebäudemanagement
- Energie, Umwelt, Infrastruktur
- Öffentliches Recht
- Gesundheit & Life Science

- Unternehmensfinanzierung
- ERP Lösungen SAP und Microsoft Dynamics AX
- IT Outsourcing und Cloud Computing

- Finanzbuchhaltung
- Lohnbuchhaltung
- Jahresabschluss und Deklaration
- Laufende Beratungsleistungen
- Tax Accounting



- Audit & Assurance
- Capital Markets & Accounting Advisory Services
- Corporate Finance
- IT-Audit & Advisory
- Sustainability Services
- **Governance, Risk & Compliance**
- Forensic Services

- Steuerberatung 4.0
- Internationale Steuerplanung
- Verrechnungspreise
- Transaktionen
- Laufende Steuerberatung
- Umsatzsteuer
- Rechtsdurchsetzung und Verteidigung
- Beratung der Unternehmerfamilie
- Vermögende Privatpersonen, Spitzensportler

BOC GROUP

Gegründet **1995 in Wien**
Spin-Off der Universität Wien

Weltweites organisches Wachstum, mit DACH-Standorten in **Wien**, **Berlin** & **Winterthur**

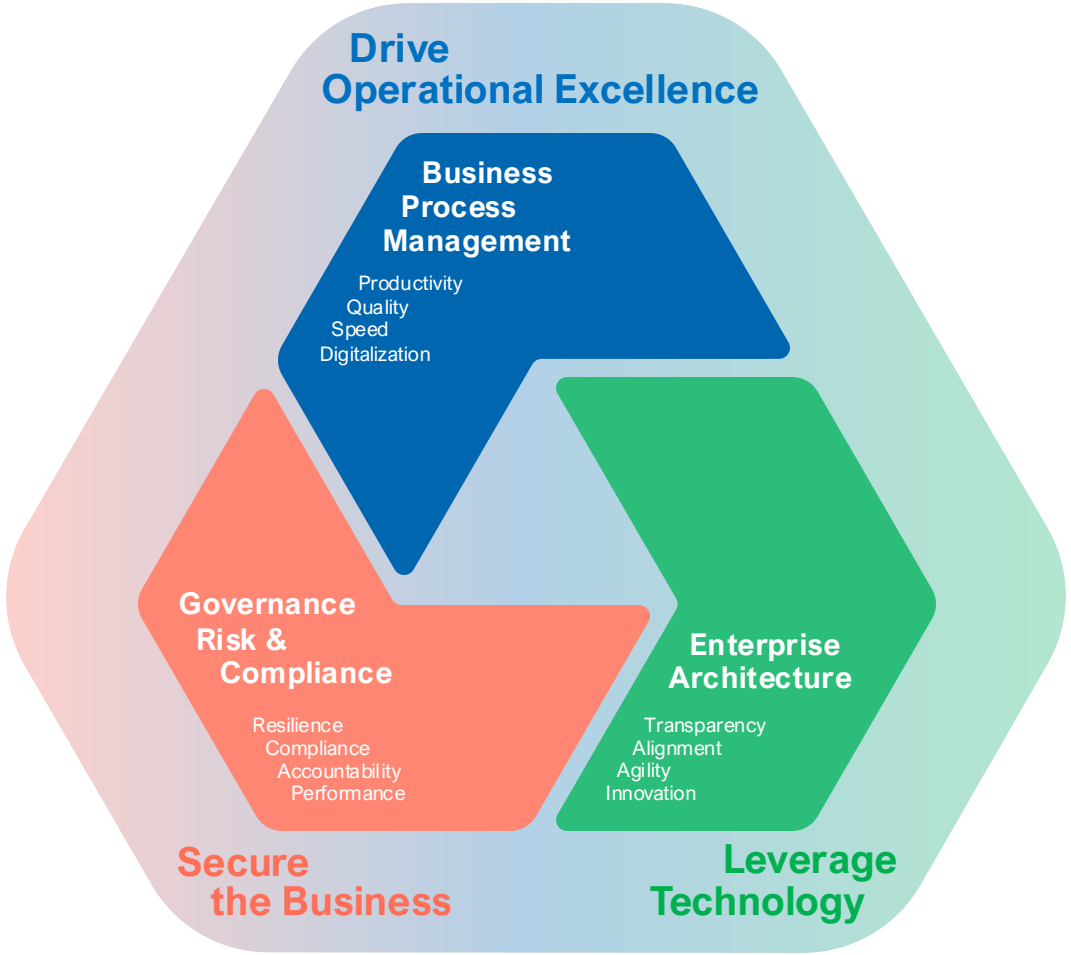
Global leader
in Modellierung & decision support systems.

BOC Group
Design Your Enterprise

We make your business run better.

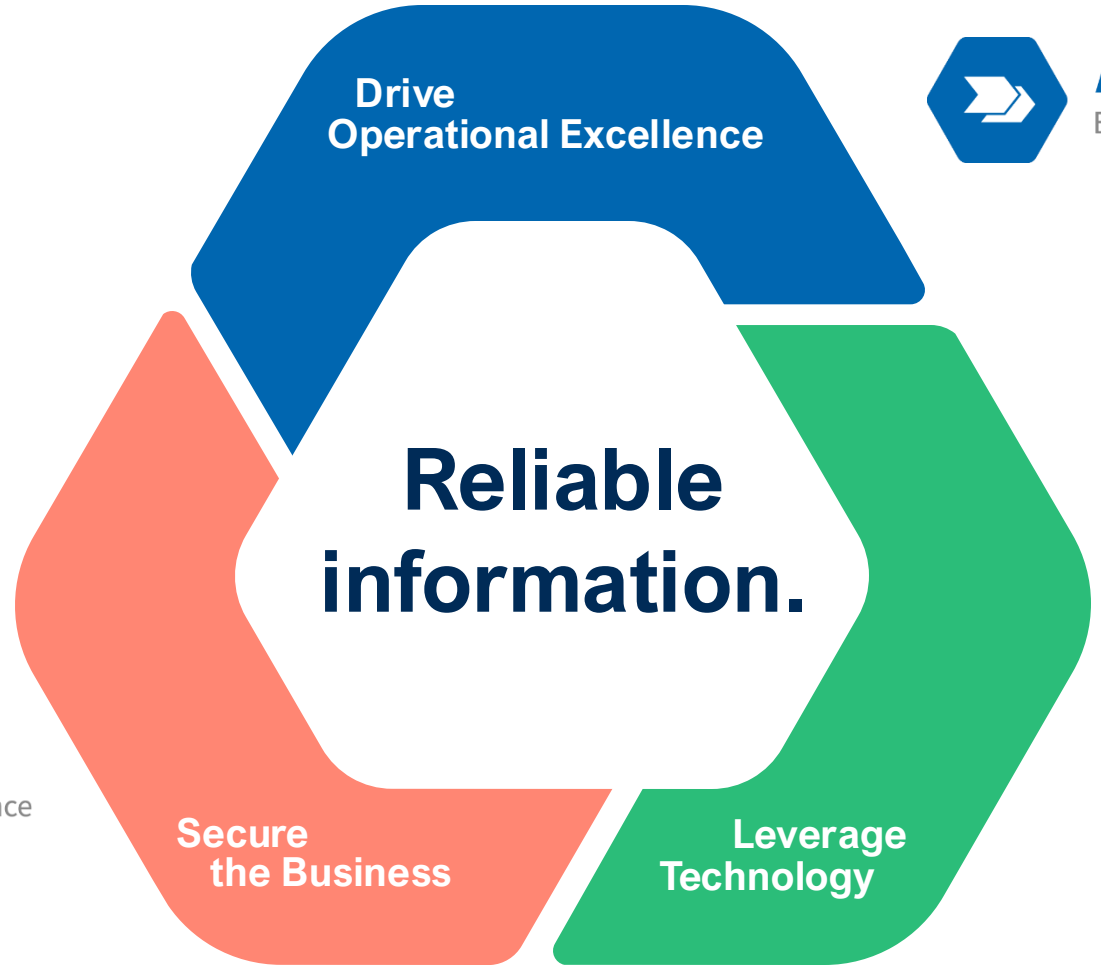
3 Fields of Action

BOC Group
Design Your Enterprise



3 Fields of Action

BOC Group
Design Your Enterprise



ADONIS
Business Transformation Suite

ADOGRC
Governance, Risk & Compliance

ADOIT
Enterprise Architecture Suite

BOC Group
Design Your Enterprise

Reliable information.
Better decisions.
Only with BOC Products.

ADONIS
Business Transformation Suite

ADOIT
Enterprise Architecture Suite

ADOGRC
Governance, Risk & Compliance

GRC SYSTEME
ERFOLGSFAKTOREN UND PRACTICAL HINTS

GRC @ RÖDL & PARTNER

„**Rödl & Partner** betrachtet GRC Fragestellungen ganzheitlich.

Ein voll *effektives GRC-System* kann nur gewährleistet werden, wenn alle Subsysteme *effektiv* und *effizient* miteinander verknüpft und koordiniert werden. Eine digitale Lösung bietet in dieser Hinsicht zahlreiche Mehrwerte.“

JAN HENNING STORBECK

Head of GRC

Compliance Management System	Risiko Management System	Internes Kontroll System	Interne Revision
IDW PS 980 n.F. ISO 37301	IDW PS 981 ISO 31000	IDW PS 982 COSO ERM	IDW PS 983 DIIR Nr.3

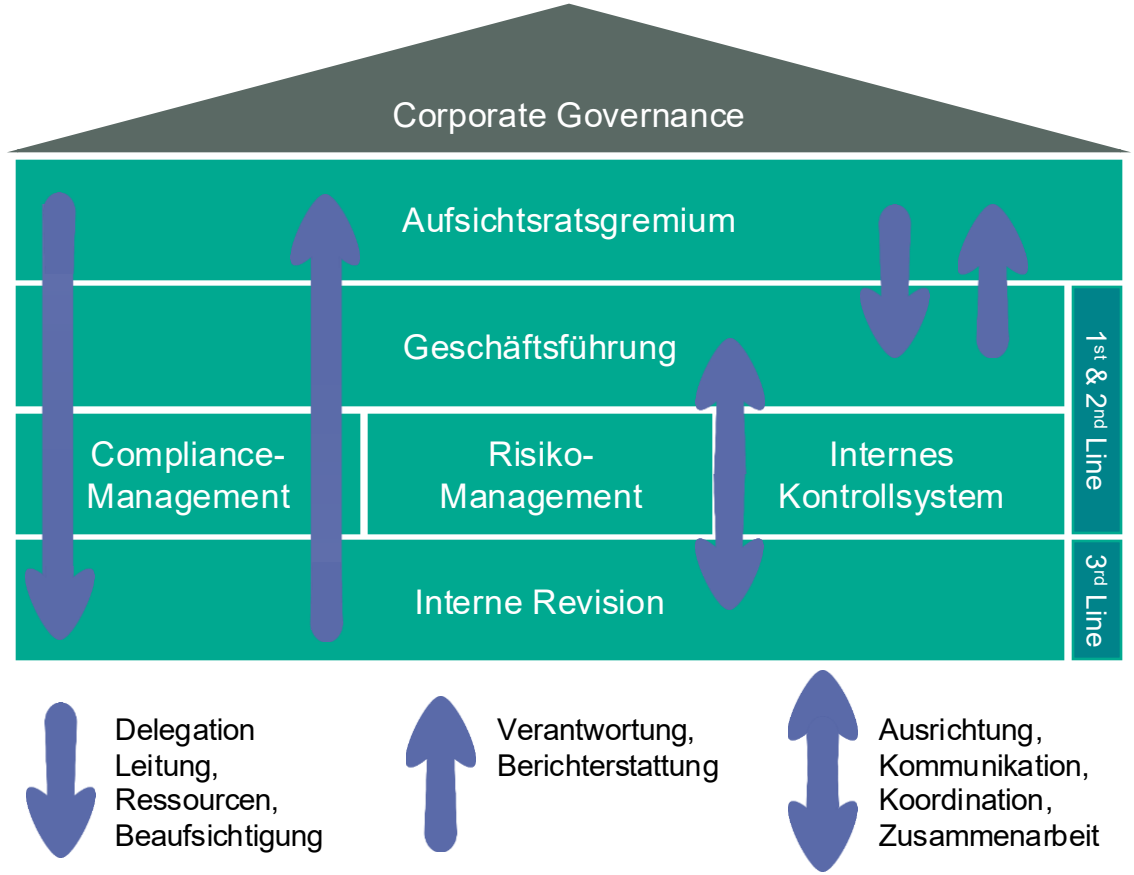
GOVERNANCE

Das House of GRC

Das House of GRC veranschaulicht die Zusammenarbeit zwischen den einzelnen Gremien und Systemen, sowie die Einbettung in das Drei-Linien-Modell des IIA.

Die Unternehmen profitieren von einem individualisierten GRC-System, das darauf abzielt, unternehmerische Risiken durch die Skalierung der gesetzlich vorgeschriebenen GRC-Aufgaben unter Berücksichtigung der Kernelemente des Drei-Linien-Modells effektiv zu steuern.

Bei der Umsetzung von Good Corporate Governance achten wir darauf, dass die Vorgaben von Gesetzgeber und Regulator effektiv und effizient umgesetzt werden.



ERFOLGSFAKTOREN UND PRACTICAL HINTS

Practical Hints	Risiko	Lösungsansatz
Trennung Internal Audit von der 1st + 2nd Line	• Rollen- und Interessenskonflikte können zu einer fehlenden Unabhängigkeit der Internen Revision führen	• Organisatorische Trennung der Internen Revision von der 1st und 2nd Line-Funktionen • Dokumentation der Unabhängigkeit im Organigramm
Unklare Berichtswege und fehlender regelmäßiger Austausch	• Risiken werden nicht an die Unternehmensleitung und andere GRC Systeme berichtet • Informationssilos und Doppelarbeit • Verlust an Effizienz und Effektivität der GRC Funktionen	• Verankerung klarer Vorgaben in einer Governance-Richtlinie mit Eskalationsmechanismen • Berichtspflichten für kritische Risiken mit definierten Berichtswegen an definierte Personen • Regelmäßige GRC Arbeitskreise zwischen 1st, 2nd und 3rd Line mit klarer Agenda und Dokumentation
Ansprechpartner / KnowHow Transfer	• Mitarbeitende kennen relevante GRC-Schlüsselpersonen nicht • Relevante Richtlinien, Arbeitsanweisungen, etc. sind nicht/schwer auffindbar im Intranet	• Zentrale GRC Homepage mit klarer Modulübersicht (u.a. „Compliance“, „Hinweisgebersystem“, „Richtlinien“, „Schulungen“) • FAQ und Quicklinks ergänzen

ERFOLGSFAKTOREN UND PRACTICAL HINTS

Practical Hints	Risiko	Lösungsansatz
Fehlende Trennung oder unklare Integration von GRC-Funktionen	• Verantwortlichkeitskonflikte oder Lücken in der Umsetzung durch unklare Systemzuordnung • Verlust an Effizienz	• Klare Ownership im Tool festlegen • GRC-Funktionalitäten je nach Organisationsstruktur integriert oder modulübergreifend implementieren
Unzureichendes Berechtigungskonzept	• Manipulation von Daten • Unautorisierte Einsichtnahme • Ggf. Verstöße gegen DSGVO	• Aufbau eines rollenbasiertes Berechtigungskonzept (z. B. Trennung je Modul, Create, Change, View, Admin, etc.) • Berechtigungskonzept ab Implementierung ausarbeiten und regelmäßiger Review der Zugriffsrechte und Accounts

ADOGRC
Governance, Risk & Compliance Suite

Securing YOUR Business. Together.

See risks clearly.
Meet compliance goals.
Ensure controls are being executed.

ADOGRC Focus Scenarios

ADOGRC
Governance, Risk & Compliance Suite

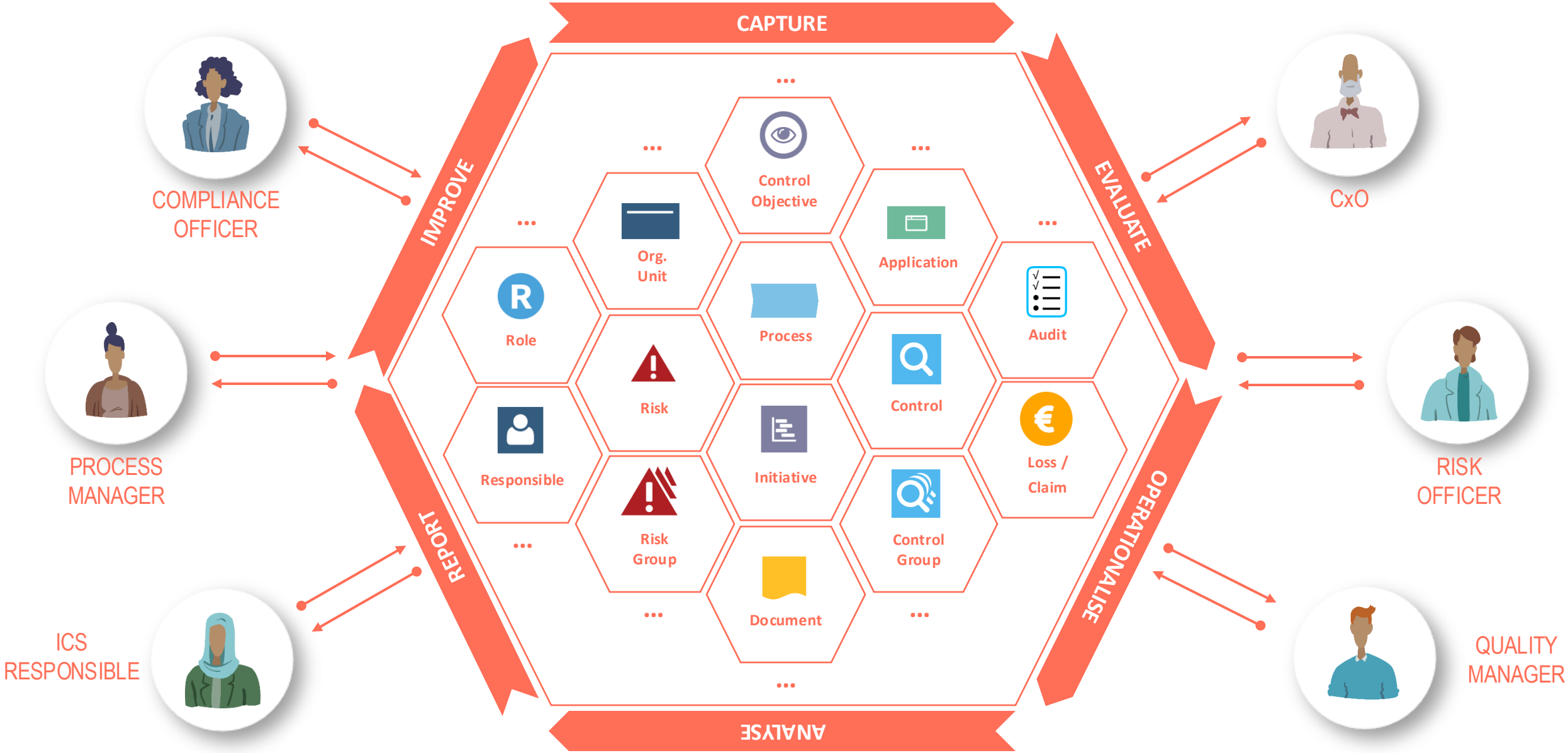
Internal Controls	Risk Mgmt.	BCM	Info- & CyberSec	Compl.	ESG	Audit	Data Prot.
COSO	ISO 31000	ISO 22301	ISO 27001	MaComp	ISO 26000	ISO 19011	GDPR
SOX	MaRisk	BSI 200-4	DORA / NIS-2	ISO 37301	UN SDGs	COBIT	RevDSG
Solvency II	FINMA	DORA	NIST / IKT	DCGK	CSDDD	COSO	NIST Priv.
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .

. . . and so much more!

***ADOGRC provides 8 Focus Scenarios**, that address specific needs, while ensuring flexibility for evolving compliance requirements.*

Rollenbasiertes Rechtekonzept

ADOGRC
Governance, Risk & Compliance Suite



ADOGRC

Your professional GRC Suite

Unified Compliance Platform

Compliance Library

Automated Workflows

Centralized Task Management

Reuse Your Trusted Data and Reliable Information to Maximize Value

... and so much more!

Securing Your Business. Together.

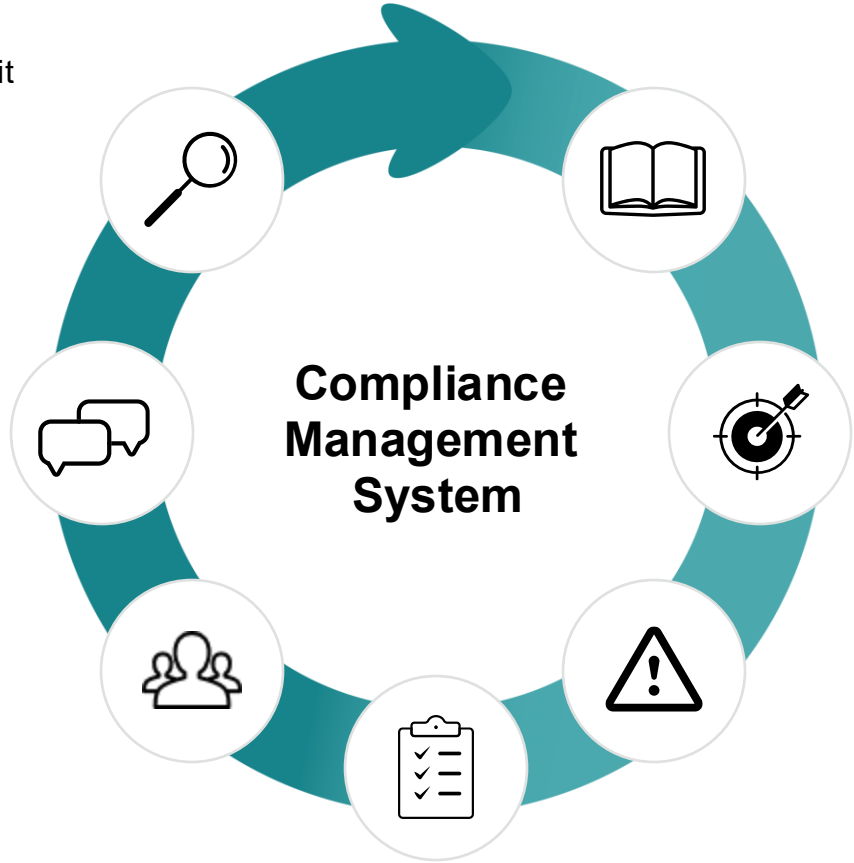
COMPLIANCE MANAGEMENT

AUFBAU DES COMPLIANCE MANAGEMENT SYSTEMS

Compliance-Überwachung und Verbesserung
- Überwachung der Angemessenheit und Wirksamkeit
- Meldung der Schwächen und Verstöße an das Management

Compliance-Kommunikation
- Aufsetzen eines Compliance Kommunikations-konzeptes
- Festlegung von Kommunikationsstrukturen
- Festlegung Berichtswege für Risiken, Regelverstöße und Hinweise

Compliance-Organisation
- Klare Abgrenzung, Kommunikation und Dokumentation von Verantwortungs-bereichen und Rollen durch das Management
- Management stellt dafür notwendige Ressourcen bereit



Compliance-Programm
- Strukturierter Ansatz um Risiken zu begrenzen
- Dadurch Vermeidung von Compliance Verstößen

Compliance-Kultur
- „Tone at/from the top“
- Grundeinstellung des Managements „Zero Tolerance“
- Beeinflusst die Mitarbeitersicht auf Compliance maßgeblich

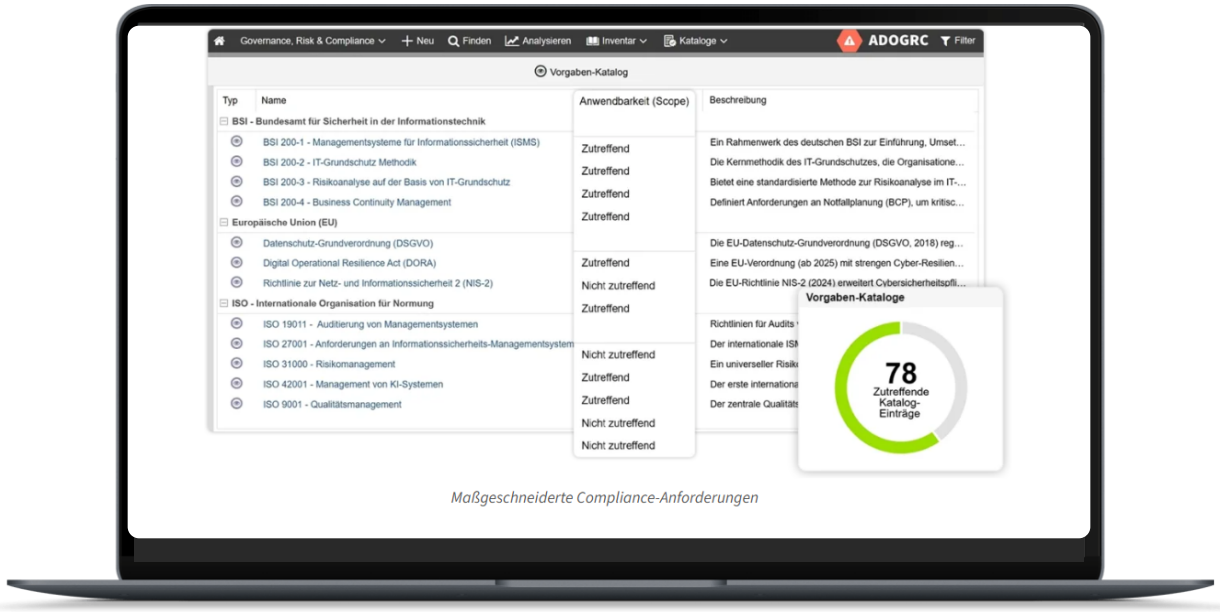
Compliance-Ziele
- Festlegung von Compliance-Zielen um die Einhaltung von Gesetzen und internen/externen Vorschriften zu gewährleisten
- Grundlage für die Beurteilung der CMS-Risken und des CMS-Programms

Compliance-Risiken
- Erhebung, Bewertung, Mitigation von Compliance Risiken
- Einführung eines Verfahrens zur systematischen Risikoerkennung

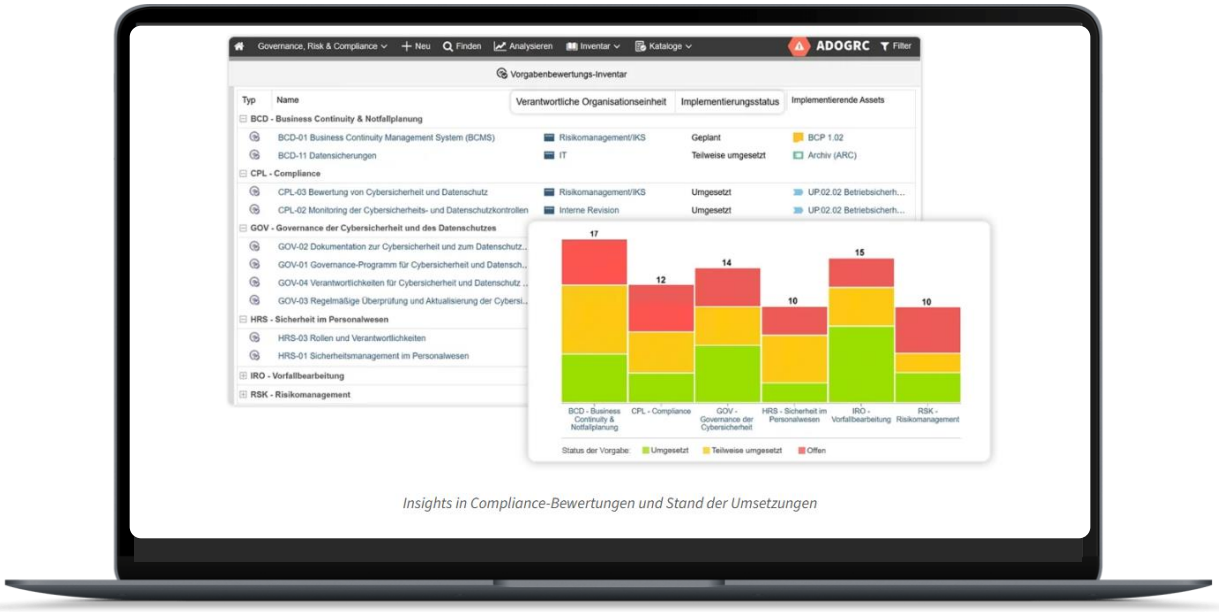
ERFOLGSFAKTOREN UND PRACTICAL HINTS

Practical Hints	Risiko	Lösungsansatz
Kommunikation und Kultur: „Tone from/at the Top“	• Fehlende Vorbildfunktion des Managements kann die Integrität und Regelakzeptanz der Mitarbeitenden negativ beeinflussen	• Verankerung von Compliance- und Risikothemen in Führungskräfteschulungen und Managementzielen • Sichtbare Kommunikation durch Geschäftsführung (Setting the Tone), Zero-Tolerance Politik
Fehlende oder unregelmäßige Schulungen	• Mitarbeitende sind nicht sensibilisiert für Risiken, Pflichten und Meldewege	• Aufbau eines jährlichen E-Learning-Programms mit Pflichtmodulen je nach Funktion • Dokumentation und Reporting der Teilnahmequoten
Ziele ohne messbare Kriterien	• Erfolgsbewertung des CMS nicht möglich	• Ziele nach SMART-Kriterien definieren (Specific, Measurable, Achievable, Realistic, Time-bound) • Regelmäßige Überprüfung und Dokumentation der Zielerreichung
Unvollständige Risikoanalyse / Rechtskataster	• Relevante rechtliche Anforderungen bleiben unberücksichtigt, mögliche Verstöße und Haftungsrisiken	• Systematisches Monitoring mit regelmäßiger Aktualisierung durch die Fachbereiche in Zusammenarbeit mit Compliance / Legal

UMSETZUNG IN ADOGRC



Maßgeschneiderte Compliance-Anforderungen



Insights in Compliance-Bewertungen und Stand der Umsetzungen

ADOGRC
Governance, Risk & Compliance Suite

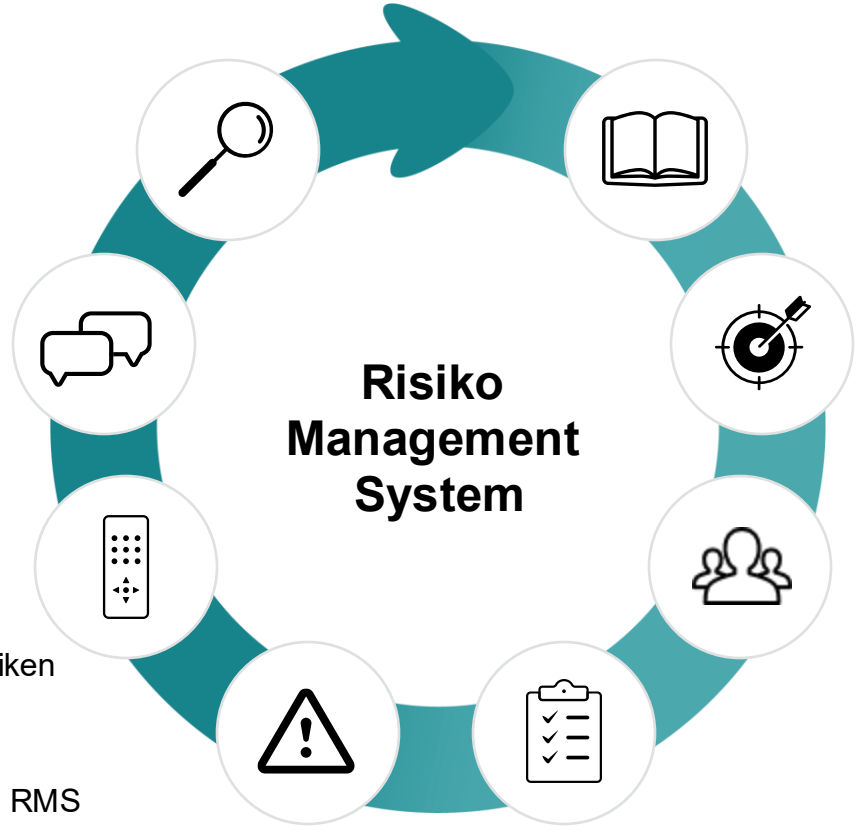
RISIKO MANAGEMENT

AUFBAU DES RISIKO MANAGEMENT SYSTEM

Überwachung & Verbesserung des RMS
- Die Angemessenheit und Wirksamkeit des RMS wird durch prozessintegrierte und prozessunabhängige Kontrollen überwacht. Festgestellte Mängel im RMS werden mit erforderlichen Maßnahmen zur Verbesserung des Systems versehen

Risikokommunikation
- Gewährleistet einen angemessenen Informations-fluss im RMS, für einen standardisierten Prozess sowie eilbedürftige Risikomeldungen

Risikosteuerung
- Auf Grundlage der identifizierten und bewerteten Risiken trifft die Unternehmensleitung Entscheidungen über Maßnahmen zur Risikosteuerung
- Als Bezugsrahmen dienen die festgelegten Ziele des RMS



Risikokultur
- Verhaltensweisen beim Umgang mit Risikosituationen sowie Risikobewusstsein im Unternehmen als Grundlage für ein wirksames RMS

Ziele des RMS
- Festlegung des Risikoappetits
- Unternehmensstrategie als Basis einer Risikostrategie für ein systematisches Risikomanagement

Organisation des RMS
- Regelung, Abgrenzung, Kommunikation und Dokumentation einer transparenten, Aufbauorganisation sowie einer klar definierten Ablauforganisation

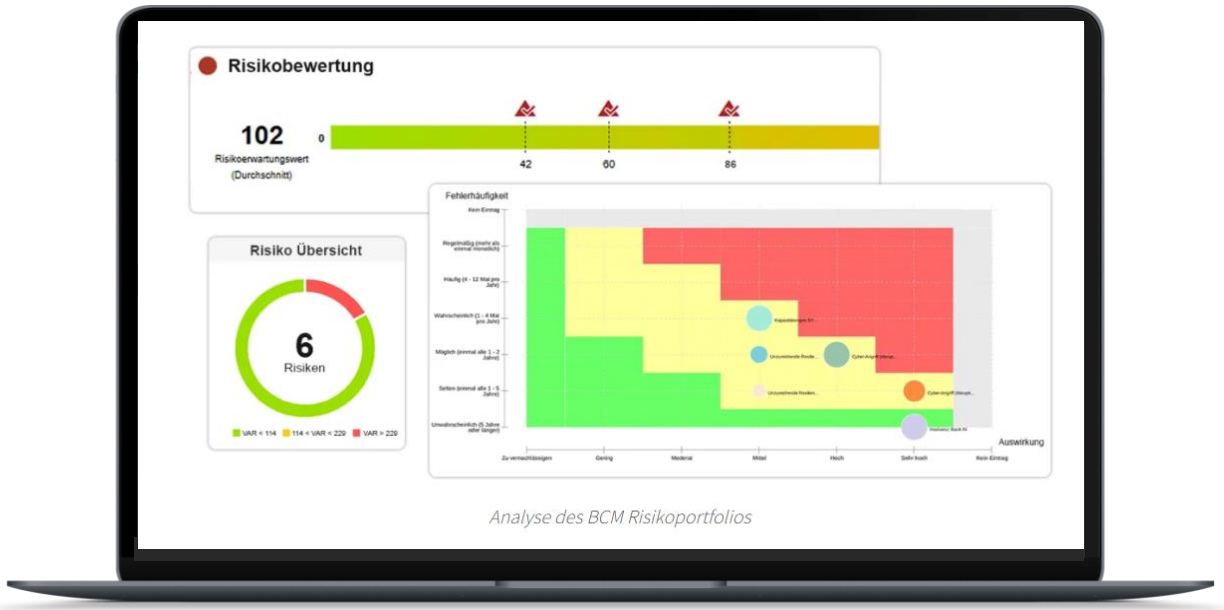
Risikobewertung
- Bewertung von Risiken hinsichtlich ihrer Eintrittswahrscheinlichkeit und möglichen Auswirkungen, einzelne Risikobewertungen werden systematisch aggregiert
- Risikointerdependenzen werden dabei analysiert und berücksichtigt

Risikoidentifikation
- Interne und externe Analyse von Entwicklungen und Ereignissen, die zu negativen oder positiven Abweichungen von den festgelegten Zielen des RMS führen können

ERFOLGSFAKTOREN UND PRACTICAL HINTS

Practical Hints	Risiko	Lösungsansatz
Fehlende Einbindung aller Gesellschaften (z. B. bei Meldungen oder Schulungen)	• Risiko fehlender Pflichterfüllung in Tochtergesellschaften • Haftungsrisiken und regulatorische Lücken	• Konzernweites GRC-Rollout mit verbindlichen Mindestanforderungen für Meldestrukturen und Schulungsteilnahmen
Kein definierter Risikoappetit / Bewertungssystem uneinheitlich	• Risiken werden nicht einheitlich priorisiert • Fokus auf irrelevante Risiken ➢ kein Steuerungseffekt	• Definition eines Risikoappetits durch das Management (qualitativ / quantitativ), inklusive klarer Bewertungskategorien (Low / Medium / High) mit Schwellenwerten
Non-Financial Risks (z. B. ESG, Reputationsrisiken) nicht berücksichtigt	• Wesentliche Risiken (z.B. Nachhaltigkeit, soziale Auswirkungen, Datenschutz) bleiben unbewertet ➢ Reputations- und Compliance Risiken	• Erweiterung der Risikoidentifikation um Non-Financial Risks • Abstimmung mit Nachhaltigkeitsabteilung • Aufnahme in das Risikoinventar
Überprüfung / Bewertung von Maßnahmen und Kontrollen findet nicht statt	• Wirksamkeit der Controls bleibt ungeprüft ➢ keine Rückschlüsse auf Verbesserungsbedarf	• Regelmäßiger Kontrollevaluierung durch die 2nd Line • Automatisiertes Maßnahmen-Tracking im GRC-Tool
Risikotragfähigkeit wird nicht ermittelt	• Es ist unklar, welche Risiken das Unternehmen ökonomisch oder strategisch tragen kann bzw. will ➢ keine fundierte Entscheidung über Risikoakzeptanz	• Definition und regelmäßige Aktualisierung einer Risikotragfähigkeitsanalyse • Ableitung eines zulässigen Gesamtrisikotragfähigkeit

UMSETZUNG IN ADOGRC



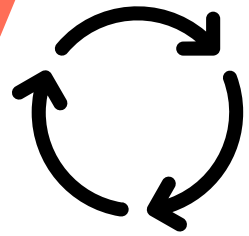
Analyse des BCM Risikoportfolios

ADOGRC
Governance, Risk & Compliance Suite

KEY TAKEAWAYS

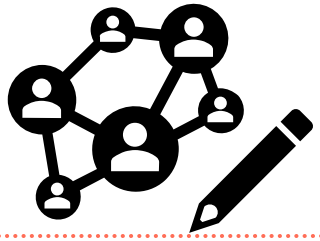
ADOGRC
Governance, Risk & Compliance Suite

1



Ganzheitlicher GRC-Ansatz (holistisch betrachten, keine Silos)

2



Schriftliche Vorgaben & Verantwortlichkeiten

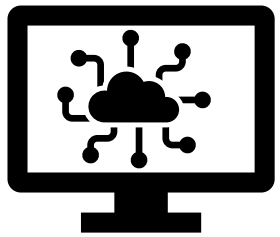
3

Risikoanalyse & -bewertung

4

Ongoing Actions (Aktualisierung, Tracking, Reporting)

5



Einsatz einer GRC-Suite (ADOGRC)

RÖDL & PARTNER GRC QUICK-CHECK

Dokumenten Review

Bereitstellung aller relevanten Dokumente (z.B. Richtlinien, Schulungsunterlagen, Kontrollen, Kommunikationsmaßnahmen) durch den Mandanten. Review und Bewertung durch die GRC Experten von Rödl & Partner.

Workshop/ Interviews

Durchführung von Experten Workshops und Interviews mit den verantwortlichen Ansprechpartner: innen des Mandanten sowie Klärung von Rückfragen aus dem Dokumenten Review.

Ergebnis Doku

Dokumentation (Management Summary) der Feststellungen und Handlungsempfehlungen aus dem GRC Quick-Check.

Wenn gewünscht, Vorstellung der Ergebnisse.

2 EXPERTEN – 1 ÜBERBLICK

Der **Rödl & Partner GRC Quick-Check** zielt darauf ab dem Mandanten einen Überblick über die **wesentlichen Handlungsfelder** der verschiedenen GRC-Themen zu geben. Hierbei kann GRC als holistisches System betrachtet (*empfohlen*) oder einzelne Bestandteile näher beleuchtet werden:

Governance	Compliance	Risiko-management	Internes Kontrollsystem
Interne Revision	HinSchG	LkSG	…

Implementierung
Beratung
Verbesserung

Prüfung und Testierung von GRC Systeme

Mehrwert

- Zugriff auf zahlreiche GRC Experten von Rödl & Partner
- Kurzfristiger Überblick über Red Flags & White Spots

Jan Henning Storbeck

Christian Uhrig

SPECIAL OFFER

ADOGRC
Governance, Risk & Compliance Suite

GRC Quick Check

Umfang

- GRC System ein Scope werden individuell mit Ihnen abgestimmt
- Review der Dokumentenlage und Workshops
- Überblick über Ihre Redflags und Whitesopts

Ihre Vorteile

- Individuelle, maßgeschneiderte Prüfung / Beratung
- Gezielte Berichterstattung
- Klare Handlungsempfehlungen

Compliance & Risk-Management in ADOGRC

Umfang

- ADOGRC Testinstanz für 2 Monate
- Inhalte aus Workshops direkt in der ADOGRC Test-Instanz aufbereitet
- Proof-Of-Value Abschlussbericht

Ihre Vorteile

- Ergebnisse können nahtlos in ADOGRC Accounts übernommen werden
- Ermittlung eines Kosten-Nutzen-Verhältnisses mit minimalem Aufwand
- Unverbindlich! Keine Lizenzkaufentscheidung erforderlich

WHAT‘S NEXT?

Live-Stream Teil 2

Jetzt **kostenlos registrieren** und die Aufzeichnung sichern!

Q&A