Versicherungsmathematisches Colloquium
Trends im Non-Financial Risk Management

Präsentation von **Claudia Meyer**
Governance, Risk, Compliance Insurance | 2025

Agenda

1	NFR-Trends	04
2	Definitionen und Methoden	07
3	NFR-Rahmenwerk und Prozesse	15
4	Typische Fallstricke im NFR und Neuausrichtung	20
5	Risikomanagement in Transformationen	23

„Das operationelle Risiko ist das Risiko eines Verlustes, das aus unzureichenden oder fehlgeschlagenen internen Prozessen, Personal oder Systemen oder aus externen Ereignissen entsteht. Diese Definition umfasst rechtliche und Compliance-Risiken, schließt jedoch strategische und Reputationsrisiken aus.“

Solvency II

NFR Trends

1

PwC Insurance Banana Skins 2025

Regulatory Change und Suitability of Regulation in Deutschland deutlich höher im Ranking

Top 10 Risiken (Global)	Rang	Top 10 Risiken (DE)
Cyber Crime	1	Cyber Crime
Artificial Intelligence	2	Technology
Technology	3	Artificial Intelligence
Macro-economy	4	Regulatory change
Climate change	5	Climate change
Regulatory change	6	Macro-economy
Human talent	7	Suitability of regulation
Change management	8	Cost reduction
Political risk	9	Political risk
Suitability of regulation	10	Change management

„Die sich rasch weiterentwickelnden Fähigkeiten im Bereich der Cyberangriffe machen es sehr schwierig, dieses Risiko vollständig zu mindern – es ist ein ständiger Wettlauf."

„Die Geschwindigkeit der KI-Einführung übersteigt die internen Kontrollen – klare Governance-, Rückverfolgbarkeits- und ethische Nutzungsrahmen sind dringend erforderlich."

„Die Entscheidung für den richtigen Ansatz in Bezug auf die technische Architektur und deren effektive Umsetzung wird für Versicherer eine Herausforderung darstellen."

Derzeitige NFR-Trends - Was beschäftigt die Risikofunktionen?

Neue Regulatorik

- ESG – Nachhaltigkeitsrisiken
- DORA*-Operationalisierung und Integration
- EU AI-Act
- Erhöhte Aufsicht und höhere Strafen
- Value for Money/ Wohlverhaltensaufsicht

Cyberrisiko und IKT-Risikomanagement

- Gefährdung von sensiblen Daten und kritischer Systeme
- Sicherheitsvorfälle bei externen Partnern
- Neue Risiken durch KI
- Stärkung des Transformationsrisiko-managements (IT-und KI-Projekte)

Risikofunktion

- Nachwuchsprobleme
- Fähigkeiten und Weiterqualifizierung
- Automatisierung und Nutzung von KI
- Etablierung einer NFR-Klammerfunktion
- Harmonisierung und Siloabbau

Geopolitik

- Ein sich schnell veränderndes Umfeld birgt Gefahr plötzlich auftretender neuer Risiken, sog. “Black Swan Events”
- Notwendigkeit von expertenbasierten Emerging Risk Assessments und Stresstestings

*DORA – Digital Operational Resilience Act

Definitionen und Methoden

2

Basel IV/Solvency II definieren sieben Arten von Ereignissen im Zusammenhang mit NF-Risiken

Durch die Beantwortung der Frage: Was ist passiert? können Sie die Art des Risikos/Ereignis identifizieren!

1. Interner Betrug
2. Externer Betrug
3. Beschäftigungspraktiken und Sicherheit am Arbeitsplatz
4. Kunden, Produkte und Geschäftspraktiken
5. Schäden an Sachwerten
6. Betriebsunterbrechungen und Systemausfälle
7. Ausführung, Lieferung und Prozessmanagement

Da zwischen den Ereignistypen und den Ursachen für die Kategorisierung operationeller/NF- Risiken eine gewisse Unschärfe besteht, verwenden viele Unternehmen ihre eigene Risikotaxonomie.

NF-Risikoereignisse können Konsequenzen in anderen Risikoarten auslösen

„Ein „boundary“ NF-Risikoereignis ist ein Ereignis, das eine Auswirkung (z. B. einen finanziellen Verlust) in einer anderen Risikoart auslöst und dort mit quantifiziert wird.“ (ORX*, 2016)

Schwierig zu identifizieren und zu quantifizieren

- Risiken der Finanzbericht-erstattung, Steuern, Nachhaltig-keitsbericht-ersattung
- Recht, Compliance, Verhaltens-risiken
- Operatives Risiko, z. B. BCM, IKT, Prozess-risiken, Resilienz-risiken, Modellrisiken
- Risiken in Trans-formations-projekten
- Boundary-Kreditrisiko
- Boundary Marktrisiko
- Boundary-Versicher-ungstech-nisches Risiko
- Boundary strategische Risiken, Geschäfts-risiken

Erfassung von Verlustdaten und Risikokontrollbewertungen (RCSA)
NFR-Universum für das interne Kontrollsystem

*ORX – Operational Risk EXchange Consortium

Die Covid-19-Pandemie ist ein NF-Risikoereignis mit Auswirkungen in vielen weiteren Risikoarten

Covid-19 Pandemie

Mitarbeitende: Körperliches und emotionales Wohlbefinden von (Schlüssel-)Mitarbeitern: Kosten für Hygienemaßnahmen, Impfstoffe

Drittparteienrisiko: Abhängigkeit von Dritten bei kritischen Prozessen und Dienstleistungen: Zusätzliche Kosten für Videokonferenzlizenzen oder höhere Systemverfügbarkeiten

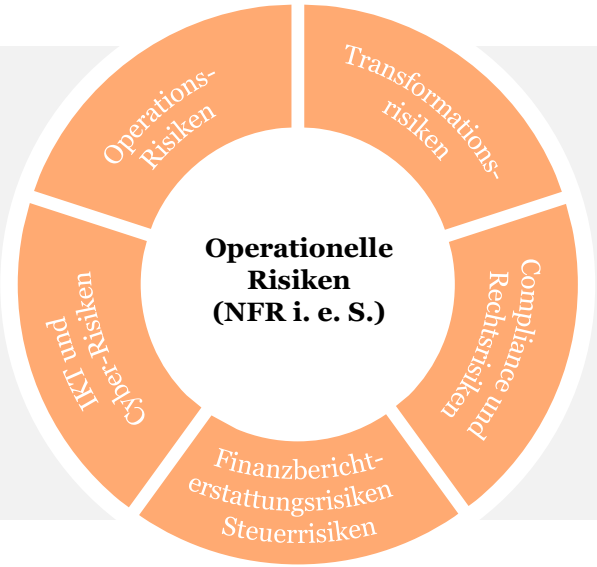
Marktrisiko: Erhöhte Marktpreisrisiken und Volatilität: Zusätzliche Absicherungskosten, ggfs. Realisierung von Verlusten

Versicherungsprodukte: Mehrdeutige Vertragsklauseln, die zu Unsicherheit und Konflikten hinsichtlich des Versicherungsschutzes führen: Entschädigungszahlungen an Kunden, Rechtskosten, Geldstrafen, freiwillige Zahlungen an Kunden

Geschäftskontinuität: Notwendigkeit, von zu Hause zu arbeiten, obwohl viele Geschäfts- und Kontrollaktivitäten für die Durchführung im Büro konzipiert sind: Kosten für zusätzliche Hardware, Software, Internet, die die Umsetzung des BC-Plans erfordern

NFR-Taxonomie deckt die komplette NF-Risikolandschaft ab, unterstützt Risikoaggregation, Analysen und die Berichterstattung

Hinweis: Nachhaltigkeitsrisiken (ESG) wirken sich auf die bekannten Risikoarten aus (Risikotreiber) und werden nicht als separate Risikokategorie betrachtet.



Risikokategorien

Kreditrisiko
Marktrisiko
Liquiditätsrisiko

Finanzielles Risko

Vers.techn. Risiken

Reputationsrisiko
Strategisches Risiko
Geschäftsrisiko
Operationelles Risiko

NFR (im weiteren Sinne)

Level 1 Risiken	Level 2 Risiken
Personal	Verstoß gegen arbeitsrechtliche oder regulatorische Anforderungen
	Unwirksame Arbeitsbeziehungen
	Unzureichende Sicherheit am Arbeitsplatz
Externer Betrug	Betrug durch Dritte/Lieferanten
	Betrug durch Vertreter/Makler/Vermittler
	Betrug durch Kunden
Interner Betrug	Interner Betrug gegen die Bank
	Interner Betrug gegen Kunden oder Dritte
Physischer Schutz und Sicherheit	Beschädigung von Sachwerten der Organisation
	Verletzung von Mitarbeitern oder Partnern außerhalb des Arbeitsplatzes
	Beschädigung oder Verletzung von öffentlichem Eigentum
Geschäfts-kontinuität	Unzureichende Geschäftskontinuitätsplanung / Ereignismanagement
Transaktions-verarbeitung und Ausführung	Verarbeitungs-/Ausführungsfehler in Bezug auf Kunden und Produkte
	Verarbeitungs-/Ausführungsfehler in Bezug auf Wertpapiere und Sicherheiten
	Verarbeitungs-/Ausführungsfehler in Bezug auf Drittparteien
	Verarbeitungs-/Ausführungsfehler in Bezug auf interne Vorgänge
	Fehler bei der Ausführung von Änderungen

Level 1 Risiken	Level 2 Risiken
Technologie	Ausfall der Hardware
	Software-Ausfall
	Ausfall des Netzwerks
Verhaltensrisiken	Insiderhandel
	Kartell- / Wettbewerbsverstöße
	Unzulässige Marktpraktiken
	Versagen des Kundendienstes (pre-sales)
	Versagen des Kundendienstes (post-sales)
	Schlechte Behandlung von Kunden / Nichterfüllung von Pflichten gegenüber Kunden
	Falsche Verwaltung von Kundenkonten
	Unsachgemäßer Vertrieb / Marketing
	Unsachgemäßes Produkt- / Dienstleistungsdesign
	Unzureichendes Whistleblowing
	Verstöße gegen den Verhaltenskodex / Code of Conduct und Fehlverhalten von Mitarbeitern

Level 1 Risiken	Level 2 Risiken
Recht	Falsche Handhabung von Rechtsverfahren
	Verletzung von vertraglichen Rechten / Pflichten
	Verletzung von außervertraglichen Rechten / Pflichten
Finanzkriminalität	Geldwäsche und Terrorismusfinanzierung
	Verstoß gegen Sanktionen
	Bestechung und Korruption
	Versagen KYC-Kontrollen und Transaktionsüberwachung
Compliance	Ineffektive Beziehung zu Aufsichtsbehörden
	Unzureichende Reaktion auf regulatorische Änderungen
	Unsachgemäße Lizenzierung / Zertifizierung / Registrierung
	Verstoß von extraterritorialen Vorschriften bei grenzüberschreitenden Aktivitäten
	Nicht-ausreichende Kapitaldeckung
Drittparteien	Schlechte Servicequalität/Serviceausfall durch Versagen der Kontrollen im Drittparteienmanagement
	Kriminelle Handlungen Dritter / Nichteinhaltung von Regeln und Vorschriften
	Unzureichende gruppeninterne Vereinbarungen / SLAs

Level 1 Risiken	Level 2 Risiken
Informations-sicherheit (einschließlich Cyberrisiken)	Datendiebstahl / böswillige Manipulation von Daten
	Datenverlust
	Cyberattacken
	Verletzung des Datenschutzes / Missbrauch der Vertraulichkeit
	Unzulässiger Zugriff auf Daten
Gesetzliche Berichterstattung und Steuern	Versagen bei der externen Finanz- und aufsichtsrechtlichen Berichterstattung
	Versäumnisse bei der Steuerzahlung/-einreichung
	Versäumnisse bei der Berichterstattung über Handel/Transaktionen
Daten-management	Nichtverfügbarkeit von Daten
	Schlechte Datenqualität
	Unzureichende Datenarchitektur/IT-Infrastruktur
	Unzureichende Datenspeicherung/Aufbewahrung und Vernichtungsmanagement
Modelle	Fehler bei der Modell-/Methodenentwicklung
	Fehler bei der Modellimplementierung
	Fehler bei der Anwendung des Modells

1

Gemeinsame Sprache sprechen

Risikoverständnis und -beschreibungen harmonisieren

2

Taxonomie

NF-Risiko-Katalog vervollständigen

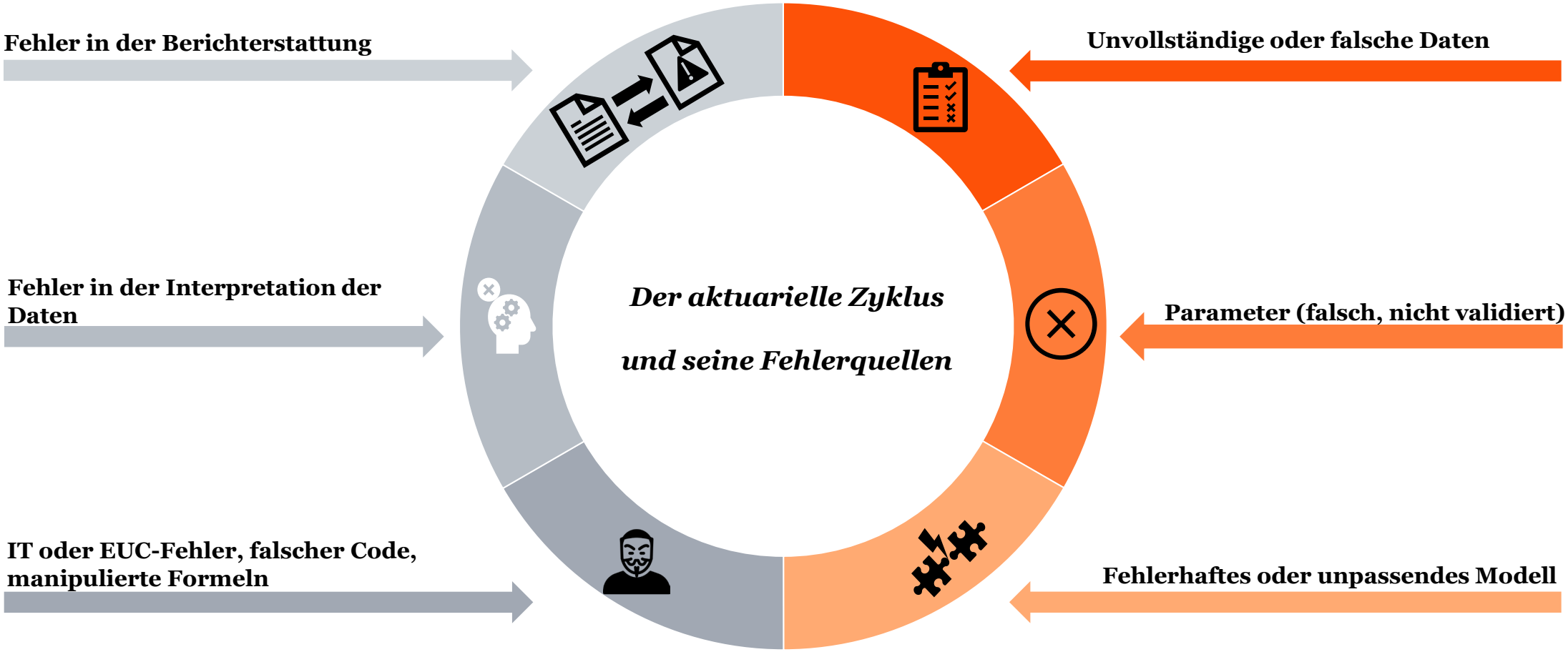
3

Mapping

Risiken den Prozessen zuordnen für klare Verantwortlichkeiten in der 1st Line

Risiken	ReWe	HR	Vertrieb	Schaden	IT	Einkauf
Interner Betrug	X	X	X	X	X	X
Betrug Kunden			X	X		
Verarbeitungsfehler	X	X	X	X	X	X
MA-Sicherheit		X				
Cyber					X	

Typische NF-Risiken im Aktuariat haben Auswirkungen auf das Pricing, die Risikokapitalberechnung, der Own Funds,…



….und sollten mit angemessenen Kontrollen mitigiert oder reduziert werden!

Operationelle Risiken haben unterschiedliche Auswirkungen

Regulatorische Auswirkungen

1 **Finanzielle Auswirkungen**

2 Reputations-auswirkungen

3 **Opportunitätskosten /entgangene Gewinne**

GuV

Beinaheschäden

Ermittlung/Schätzung der Auswirkungen in den RCSA und Szenarioanalysen

- Behördliche Geldstrafen
- Verluste aufgrund krimineller Aktivitäten, wie z. B. Betrug
- Kosten im Zusammenhang mit Ermittlungen und Rechtsanwälten
- Kosten im Zusammenhang mit der Wiederherstellung des vorherigen Status
- Entschädigungszahlungen an Kunden

- Sinkender Markenwert – höhere Kapitalisierungskosten (Herabstufung des Ratings)
- Rückgang des Aktienkurses (meist nur kurzfristig)
- Kundenweggang
- Negative Presse
- Anfragen/Prüfungen durch Regulator

- Entgangene Erträge aufgrund von Systemunterbrechungen (z. B. Online-Portale)
- Opportunitätskosten bei Systemausfällen, da Mitarbeiter nicht arbeiten können

Typische Risikobewertungsmethoden für NFR

Best Practice

- Es existiert eine einheitliche Risikobewertungsmethode (inhärent und residual) für alle NFR-Arten.
- Nutzung von internen und externen Verlustdaten helfen bei der Expertenschätzung
- Risikoappetit definiert u. a. Etablierung von Kontrollen und Maßnahmen in der 1st Line – und somit die Risk Response.
- Es existiert auch eine harmonisierte Bewertungsmethode für Verlustereignisse, IKT-Vorfälle (DORA), Compliance Issues, Feststellungen und Kontrollschwächen.

Finanzielle Auswirkung

Eintrittswahrscheinlichkeit: Rating	0–10k	10–100k	100k–500k	500k–2 Mio	>2 Mio.
<10%	sehr niedrig	sehr niedrig	sehr niedrig	sehr niedrig	niedrig
10%–50%	sehr niedrig	niedrig	niedrig	niedrig	moderat
50%–70%	niedrig	niedrig	moderat	moderat	hoch
70%–90%	moderat	moderat	hoch	hoch	sehr hoch
>90%	hoch	hoch	hoch	sehr hoch	sehr hoch

Risikoappetit

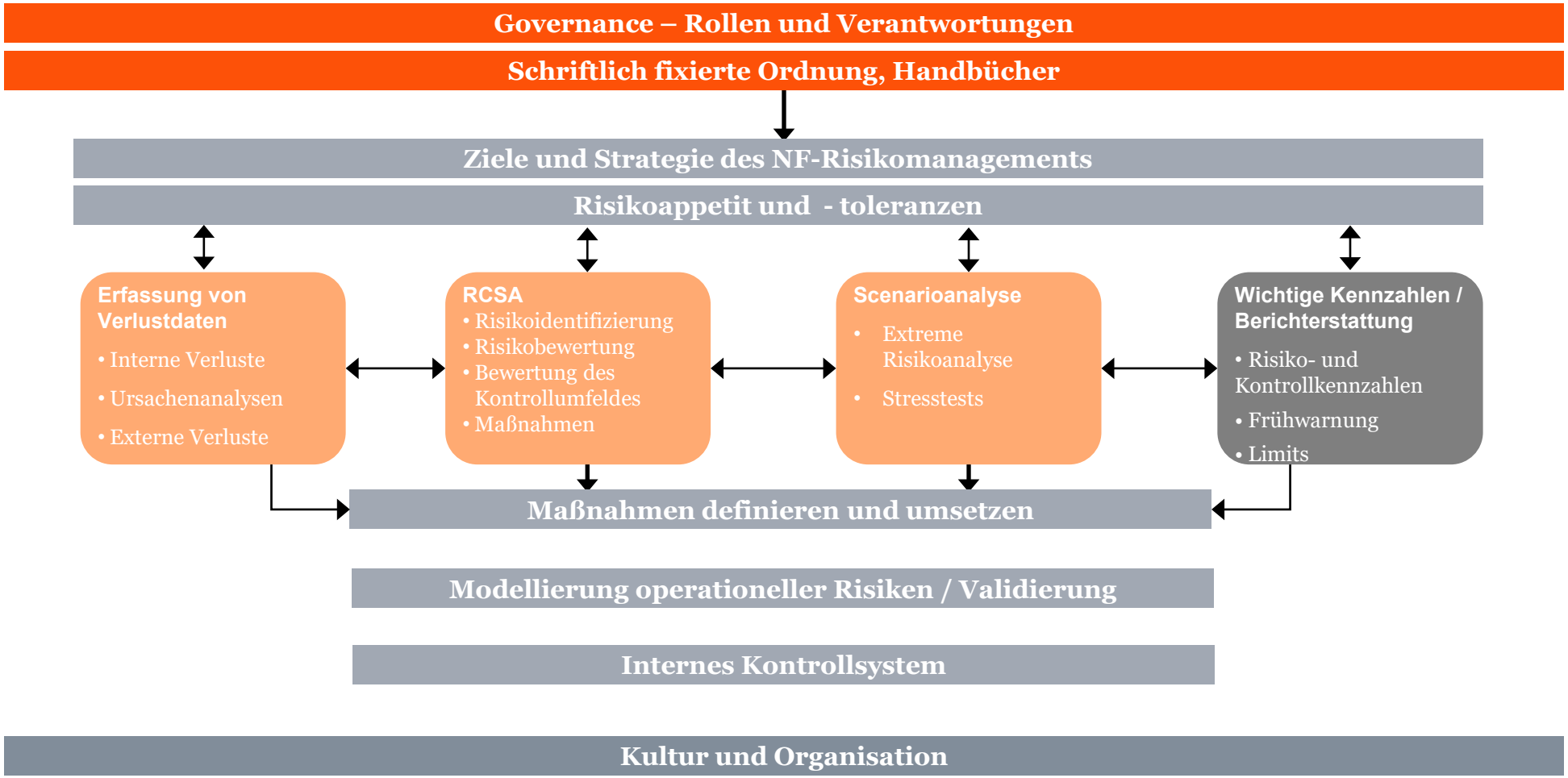
Nicht-finanzielle Auswirkung (RepRisk)

Rating	Stake-holder Aufmerk-samkeit	Kriterien zur Bewertung der Auswir-kungen auf die Stakeholdergruppen			
		Investoren	Kunden	Regulatoren	…
sehr niedrig					
niedrig					
mittel					
hoch					
sehr hoch					

NFR-Rahmenwerk und Prozesse

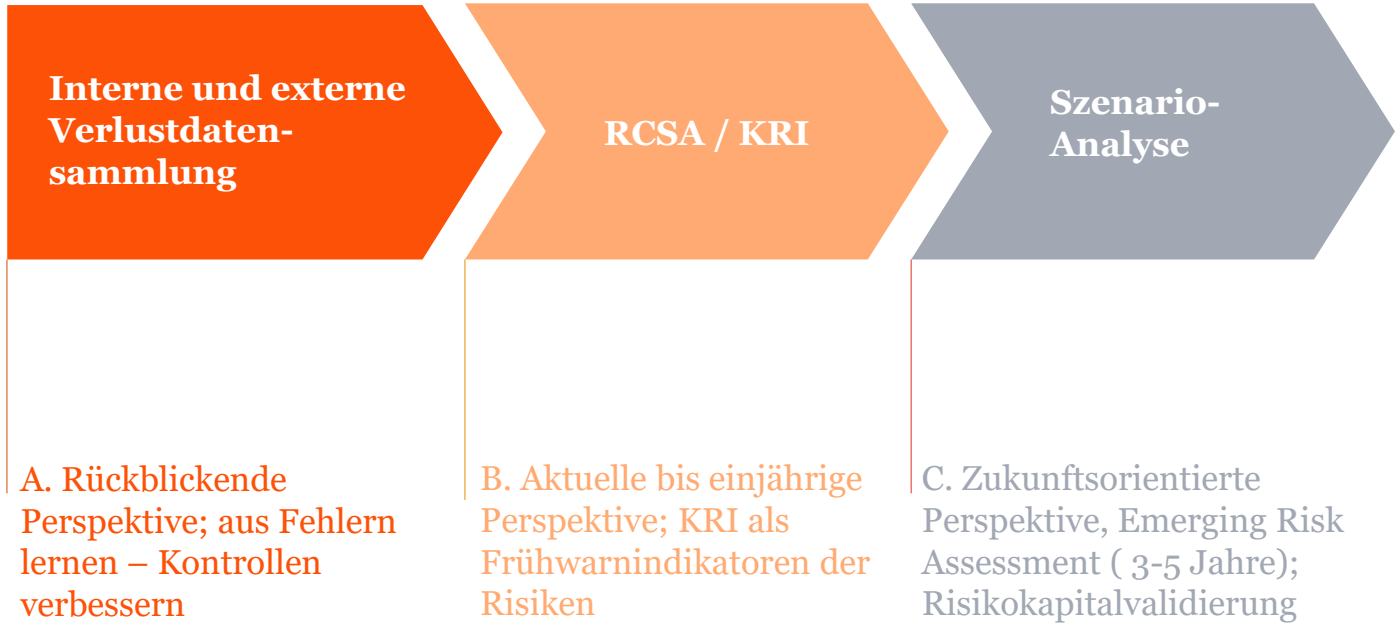
3

Elemente und Prozesse des NFR-Rahmenwerks stärken klare Verantwortlichkeiten



Prozesse zur Risikoidentifizierung, -bewertung und -steuerung

Die Identifizierung und Analyse von NF-Risiken zielt darauf ab, die Risiken sowohl aus einer vergangenen, aktuellen als auch aus einer zukunftsorientierten Perspektive zu analysieren und pro-aktiv zu steuern.



Beispiel eines typischen, jährlichen NF-Risikosteuerungskreislauf

1 Aktualisierung/Scoping Q4/Q1 (NFR mit Risikospezialfunktionen und IKS)

- Überprüfung/Ergänzung des Risikokatalogs
- Zuordnung von Risiken zu Prozessen prüfen
- Entwicklung von neuen Schlüsselkontrollen/Kontrollzielen
- Überprüfung der Risikotoleranzen
- ggf. Bestimmung der jährlichen Schwerpunktthemen, u. a. für Kontrolltesting, Risk Deep Dives

2 Bewertung von Risiken und dem Kontrollumfeld/alle NFR gemeinsam Q1/Q2 (1st Line)

- regelmäßige und Ad-hoc-Risiko- und Kontrollbewertungen (Transformation und BAU)
- Identifikation und Implementierung von Maßnahmen bei Überschreitung der Toleranz
- Aktualisierung von Kontrollen
- Identifikation und Überprüfung von KRIs

3 Kontrolltestings Q3/Q4 (NFR und IKS mit Risikospezialfunktionen)

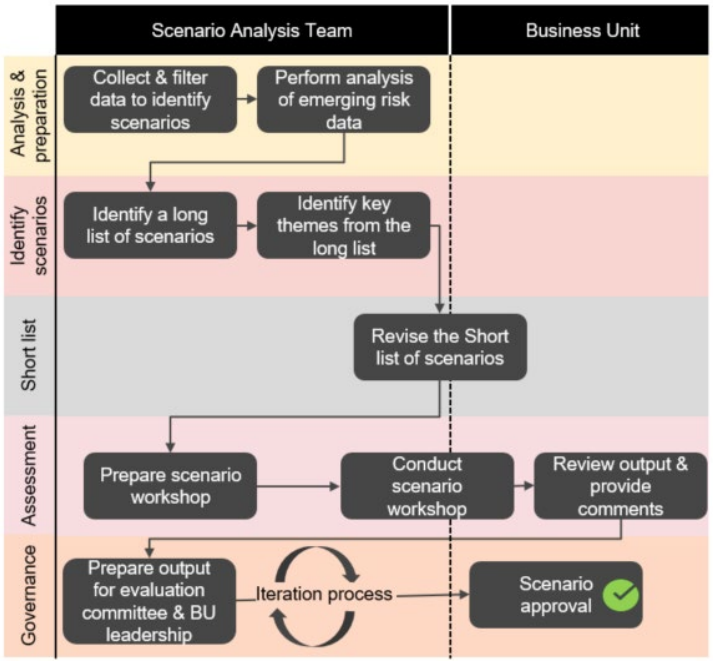
- Erstellung eines umfassenden Testplans (basierend auf dem Revisionsplan)
- Durchführung von unabhängigen Kontrolltests
- Konsolidierung von Testergebnissen
- Umsetzung von Maßnahmen bei Kontrollschwächen (1st Line)

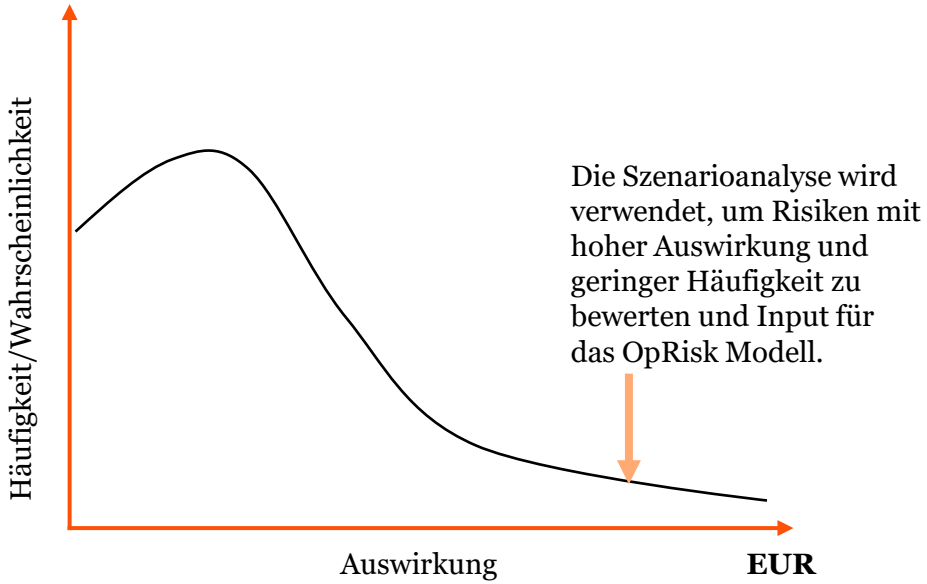
4 Risikoberichterstattung und -überwachung (laufend) (NFR)

- Überwachung von KRIs
- Überwachung von Maßnahmen
- regelmäßige Berichterstattung

Expertenbasierte Szenario-Analyse für die untenehmensweite Risikosteuerung und Validierung der Kapitalzahlen

„Die Szenarioanalyse ist ein Prozess, bei dem **Expertenmeinungen** von Führungskräften der ersten und zweiten Ebene eingeholt werden, um **potenziell, neue operationelle Risiken** zu identifizieren und **deren mögliche Folgen unternehmensweit** zu bewerten. Die Szenarioanalyse ist ein **wirksames Instrument**, **um potenzielle Quellen für erhebliche NF-Risiken** und den Bedarf an zusätzlichen Kontrollen oder Maßnahmen zur Risikominderung zu identifizieren. Angesichts der Subjektivität der Risikobewertung (Daten sind z.T. nicht vorhanden) sind ein robustes Governance-Rahmenwerk, die Identifizierung von Risikotreibern sowie eine Expertenausbildung zum Thema „Biases“ unerlässlich, um die Integrität und Konsistenz des Prozesses sicherzustellen.“

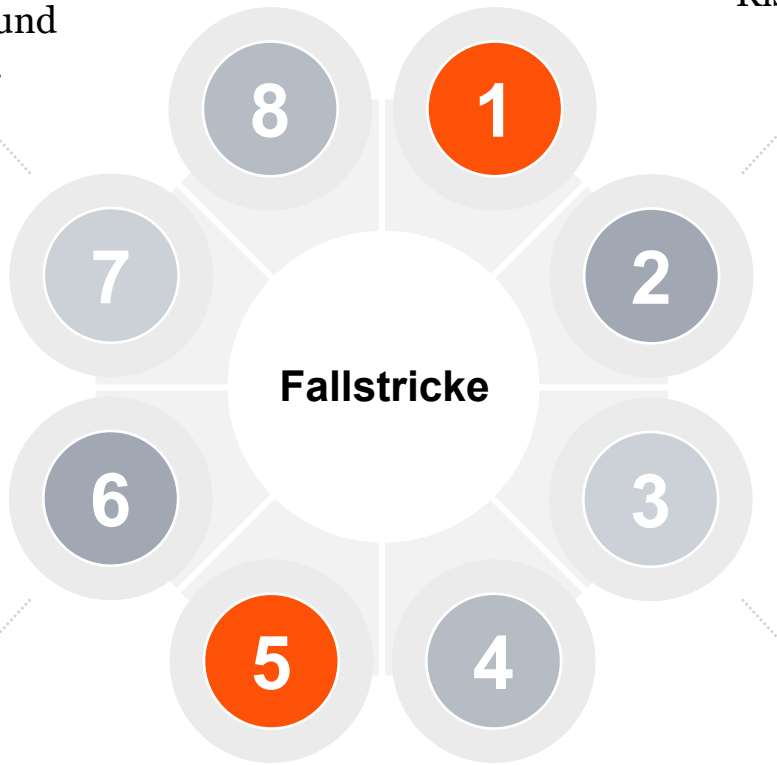




Typische Fallstricke im NFR-Management und Neuausrichtung NFR

4

Fallstricke im NFR-Management



1. Risikofunktion nicht in Transformation und Wandel eingebunden; nur reaktive Risikokontrolle bei BAU-Prozessen
2. Unklarer Risikoappetit und fehlende Toleranzschwellen für die Umsetzung interner Kontrollen
3. Nicht integrierte OpRisk-Methodik, Management, Kontrolltests und Berichterstattung; Risikofunktion fungiert nicht als „Klammerfunktion“
4. Fehlende Ursachenanalyse interner und externer Verlustereignisse; kein Lernen aus Fehlern
5. Mangelnde Kapazitäten und Kenntnisse im NFR-Team – erlaubt nur reaktives statt aktives RM
6. Fehlende regelmäßige Szenarioanalyse von Black-Swan-Ereignissen und voreingenommene („biased“) Experten
7. Fehlendes GRC-System und schlechte Qualität oder unvollständige Risikodaten sowie fehlende „So what”-Empfehlungen an die Vorstände
8. Risikomanager stellen Risikobewertungen der 1. Verteidigungslinie nicht in Frage und führen sie auch nicht gemeinsam durch.

Strategische Neuausrichtung der NFR-Funktion

„Build robots for day-to-day risk management and hire hunters to detect new and emerging risks“

Harmonisierung

- Harmonisierung der Risikobewertungsmethoden ist eine Vorrausetzung für die Vergleichbarkeit und Steuerung aller NF-Risiken
- Ganzheitliche Steuerung und Überwachung aller OpRisks gebündelt, z. B. in einem NFR-Komitee
- Harmonisierung der Berichterstattung zur besseren Entscheidungsfindung durch den Vorstand

Automatisierung

- Datengestützte Risikobewertung
- Automatisierte Analysen und Berichte
- Einsatz eines integrierten GRC- Systems für die 1., 2.und 3. Verteidigungslinie

Verknüpfung mit IKS und IKT-Management

- OpRisk Risikoappetit/-toleranz bestimmt das Implementieren von Kontrollen im Business.
- Eine integrierte Risiko- und Kontrolltaxonomie gemappt auf die Geschäftsprozesse erleichtert das Identifizieren und Managen von Risiken im Business.
- Die Überwachung von internen und externen Faktoren (z. B. Regulatorik) stellt sicher, dass das Risikoprofil aktuell ist und die Kontrollen zeitnah angepasst werden.

Freisetzung von Ressourcen in der Risikofunktion durch Harmonisierung und Automatisierung – Nutzung der freien Kapazitäten für aktives Risikomanagement in Transformationen und für unabhängiges Kontrolltesting

Verschlankung der Risikoprozesse in der 1. Verteidigungsline führt zu weiteren Kosteneinsparungen.

Risikomanagement in Transformationen

5

Gründe für ein systematisches Transformationsrisikomanagement

Kunde

- Mindestens gleiche Servicequalität während der Umstellung und bei der Inbetriebnahme
- Bessere Kunden- und Mitarbeitererfahrung nach der Inbetriebnahme

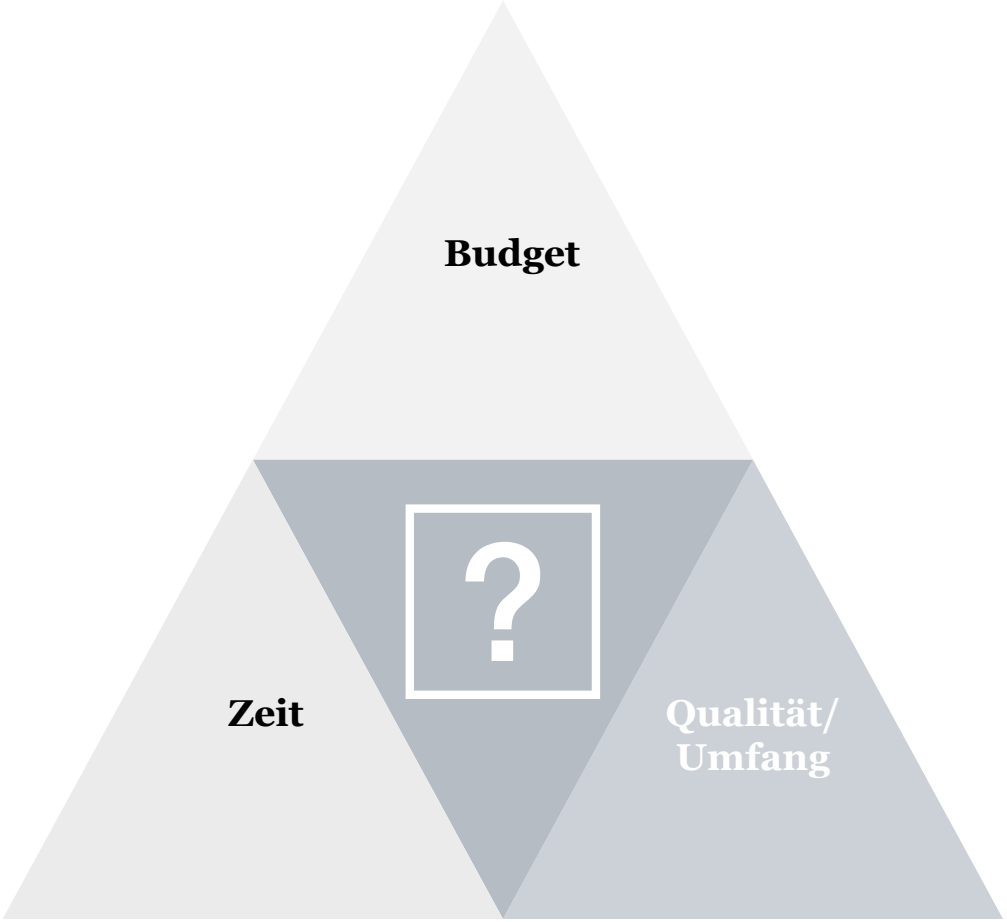
Aufsicht

- Einhaltung oder Umsetzung von Governance-Vorgaben
- Integration der zweiten Verteidigungs-linie für das Risikomanagement
- Fokus auf KI, IKT-, Outsourcing und Regulatorik-Projekte

Unternehmen

- Bessere und transparente Projekt-steuerung, Vermeidung von massiven Budgetüberschreitungen
- Steigerung der Effizienz im „Future BAU”
- Automatisierung der Kontrollen
- Erhalt des Franchise-Values

Projektziele sind auch Projektrisiken – das magische Dreieck der Transformation



Zwei Arten von nichtfinanziellen Risiken müssen während der Transformation gesteuert werden

1 Transformations-/Projektrisiken

- Zeit, Budget, Umfang
- Betriebsrat
- Reputation
- ESG
- Gesetzliche Änderungen
- Technologische Risiken
- Off-/Nearshoring
- Projektabhängigkeiten, usw.

2 Risiken des künftigen BAU nach Go-Live

- IKT und KI-Risiken
- Datenschutzrisiken
- Risiken im Zusammenhang mit der Aufbewahrung von Daten und Dokumenten
- Compliance- und Rechtsrisiken
- Steuerrisiken
- BCM-Risiken
- Risiken im Zusammenhang mit Service providern
- Prozessrisiken
- usw.

Verzahnung des Risikomanagmentprozesses in den Transformationsprozess

Projektauswahl

- Definition der „im Umfang enthaltenen“ Projekte
- Die Risikofunktion sollte aktiv auf PMO, COO usw. zugehen, um Projekte für die Beteiligung der zweiten Linie auszuwählen

Planung

- Die Risikofunktion muss den Projektinhalt verstehen
- Erste Risikoeinschätzungen vornehmen

Workshop

- Projektleiter (PL) treibt den Prozess
- Risikofunktion berät und hinterfragt
- Gemeinsame Identifizierung und Bewertung von Risiken
- PL plant Maßnahmen und definiert KPIs

Reporting

- Risikobewertungs-ergebnisse an den Lenkungsausschuss melden, ggfs. Vorstellung im Risikokomitee
- Maßnahmen beschließen

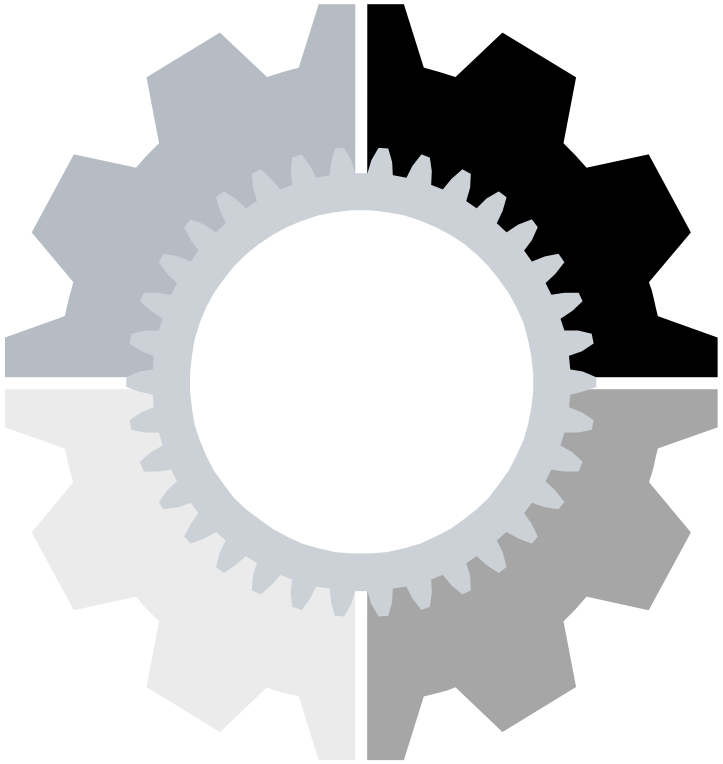
Update

- Mindestens alle 6 Monate
- Oder bei größeren Änderungen des Umfangs
- Anpassung an Sprints
- Überwachung der Maßnahmen und der KPIs

Entscheidende Erfolgsfaktoren im Projektrisikomanagement

- Risikofunktion als „Partner“ des Projektmanagers
- Einbeziehung anderer Fachexperten (Compliance, InfoSec, Rechtsabteilung, Steuerabteilung)
- Beraten und Hinterfragen
- Gemeinsamer Risiko-Workshop

- Risiko-Workshop bereits in der Planungsphase durchführen
- Budgetplanung umfasst auch die Automatisierung von Kontrollen
- Verwendung der bisherigen RCSA-Ergebnisse für die BAU-Risiken



- Projektmanagement-Rahmenwerk
- Verantwortung in der ersten Linie
- Projektmanager-Schulung zu Risikomanagement
- „Lessons learned“ nach Go-Live

- Nutzung des Risikokataloges/Taxonomie
- Weniger Bewertung – mehr Fokus auf Maßnahmen und Kontrollen sowie KPIs
- Anpassung und Implementierung von Kontrollen vor der Inbetriebnahme
- Freigabe zur Inbetriebnahme durch alle Stakeholder und umfangreiche Mitarbeiterschulungen

Ihre Ansprechpartnerin

Claudia Meyer

Senior Manager
Governance, Risk, Compliance
Versicherungen

claudia.meyer@pwc.com
+49 160 96558100

Vielen Dank für Ihre Aufmerksamkeit.

Q&A

pwc.de

© 2025 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.
Alle Rechte vorbehalten. "PwC" bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.