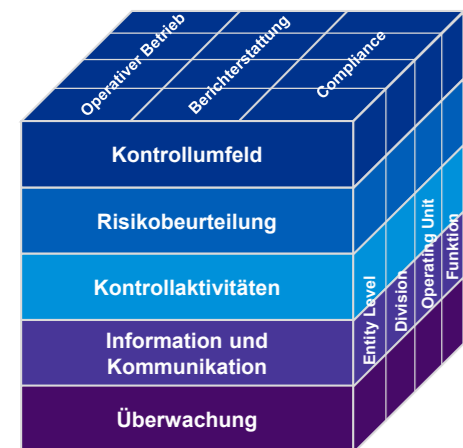




# Mit Effizienz & Sicherheit - unsere Ansätze für die Ausgestaltung des Internen Kontrollsystems (IKS) im Financial Services-Umfeld

## Definition des Internen Kontrollsystems



Das unternehmensweite interne Kontrollsystem ist die Gesamtheit aller systematisch gestalteten **Kontrollen** und **organisatorischen Maßnahmen** im Unternehmen zur **Erreichung der Unternehmensziele** und zur **Abwehr von Schäden**:

- Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (**Operativer Betrieb**)
- Ordnungsmäßigkeit und Verlässlichkeit der externen und internen Rechnungslegung (**Berichterstattung**)
- Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften (**Compliance**)

Aus: COSO Rahmenwerk „Internal Control – Integrated Framework (2013)“ des Committee of Sponsoring Organizations of the Treadway Commission (COSO); allgemein anerkanntes Konzept hinsichtlich der Gestaltung des Internen Kontrollsystems (IKS)

## Regulatorische Grundlagen



Den übergreifenden Rahmen für das IKS im FS-Umfeld bilden insb.

- § 91 (2) und § 107 (3) AktG
- die IDW Prüfungsstandards PS 261 und 951
- der Deutsche Corporate Governance Kodex

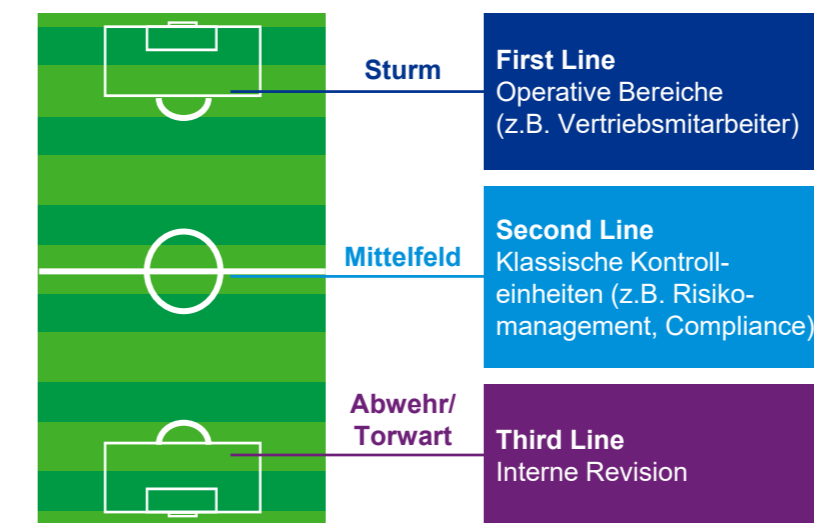
Daneben existieren verschiedene branchenspezifische Ergänzungen (Auswahl):

- Banken: § 25 a KWG, MaRisk AT 4.3 und EBA Guidelines on Internal Governance
- Versicherungen: § 29 VAG und MaGo Abs. 12
- Asset Manager: § 28 KAGB und 4.3 KAMaRisk

## Das IKS erstreckt sich auf alle Bereiche des Unternehmens

„**Three Lines**“ als Rahmenwerk für ein ganzheitliches Governance-System

- Förderung eines systematischen Ansatzes zur Identifikation und Handhabung von Unternehmensrisiken und zur Erreichung von Unternehmenszielen
- Leitlinien für eine systematische Organisation der Akteure und Komponenten zur Risikoüberwachung auf drei voneinander unabhängigen Ebenen unterhalb der Unternehmensleitung
- Einbettung der einzelnen Kontrollfunktionen in ein ganzheitliches Governance-System



### „Die Abwehr beginnt im Sturm“

Die 1st Line (operative Geschäftsbereiche) ist für die Dokumentation von Prozessen und die Einrichtung angemessener und wirksamer Kontrollen verantwortlich.

Die 2nd Line (Risikomanagement, Compliance, weitere Kontrollfunktionen) ist für die unabhängige Überwachung der 1st Line hinsichtlich der Angemessenheit und Wirksamkeit verantwortlich.

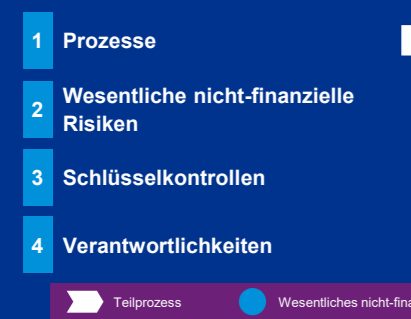
Die 3rd Line (Interne Revision) agiert als prozessunabhängige Prüfungsinstanz des IKS über alle Einheiten des Unternehmens hinweg.

## Der IKS-Regelkreis dient zur Sicherstellung von Vollständigkeit und Aktualität sowie Angemessenheit und Wirksamkeit des unternehmensweiten IKS

### Die Identifikation wesentlicher Risiken erfolgt entlang der E2E-Prozesse

Mittels einer End-2-End-Prozessbetrachtung wird die vollständige, konsistente und redundanzfreie Identifikation und Bewertung wesentlicher nicht-finanzieller Risiken sichergestellt.

#### Ablauf der Prozess-Risikoanalyse



#### Kernfragen der Prozess- Risikoanalyse

Welche relevanten Prozessschritte gibt es im Prozess?  
Welches sind die wesentlichen nicht-finanziellen Risiken im Prozess?  
Welche Schlüsselkontrollen sind zur Mitigation dieser Risiken erforderlich?  
Wie sind die Verantwortlichkeiten definiert? (Kontrolldurchführung, Teil- und Gesamtprozess, Kontroll-Processdesign)

### Die Konzentration auf Schlüsselkontrollen für wesentliche Risiken ermöglicht eine stringente Fokussierung

Einheitliche Erfassung, Bewertung und Dokumentation von prozessintegrierten Kontrollaktivitäten je wesentlichem Risiko.

Prozess-ablauf	Teilprozesse, Subprozesse, Prozessaktivitäten	Kontrollziel	Was soll mit der Kontrolle erreicht werden?
Wesentliche Risiken	Operationelle, Compliance, Financial Reporting Risiken	Kontroll-aktivitäten	Wie läuft die Kontrolle genau ab?
Kontrollen	Verortung von Schlüsselkontrollen für wesentliche Risiken	Kontrolltyp	Checkliste, Vier-Augenprinzip, Plausibilisierung etc.
Verantwort-lichkeiten	Prozesse, Kontrollen, Auslagerungen	Frequenz/Zeitpunkt	Täglich/wöchentlich/monatlich/jährlich, vor-/nachgelagert
Weitere Angaben	Involvierte IT-Systeme, Auslagerungen, Vertriebskanäle	Eskalations-prozess	Beschreibung des Umgangs mit Kontrollfeststellungen

### Das Ergebnis des IKS-Regelkreises ist ein aussagekräftiges Reporting an Aufsichtsrat und Vorstand

Angemessenheits- und Wirksamkeitsbestätigung in einem IKS-Bericht, im Idealfall in Zusammenarbeit mit anderen Kontrollfunktionen zur Sicherstellung einer konsistenten und redundanzfreien Berichterstattung zur Risikosituation des Unternehmens.

#### Adressaten und Herausforderungen des IKS-Reportings

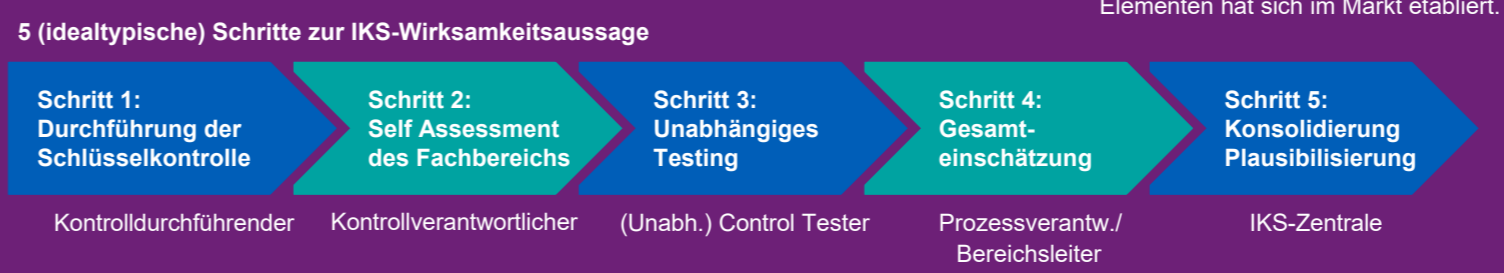
- Adressaten
  - Aufsichtsrat: als Grundlage für die jährliche Wirksamkeitsaussage
  - Vorstand: zur Information über den Zustand des IKS im gesamten Unternehmen
  - Berichtslinien: zur Information über den Zustand des IKS in ihrem Bereich
  - Reporting muss je nach Empfänger unterschiedliches Granularitätslevel haben
- Wesentliche Herausforderungen
  - Reichweite der Aussage zur Angemessenheit und Wirksamkeit des IKS
  - Sicherstellung der Konsistenz und Belastbarkeit des Reportings
  - Vergleichbarkeit des Reportings mit „Aussagen“ anderer Kontrollfunktionen

#### Ampelelogik

- das IKS ist (überwiegend) nicht angemessen und/oder nicht wirksam
- das wesentliche Risiko ist durch IKS-Schlüsselkontrollen in einigen Fällen nicht reduziert
- das IKS ist überwiegend angemessen und wirksam
- das wesentliche Risiko ist durch IKS-Schlüsselkontrollen nicht in allen Fällen reduziert
- das IKS ist weitgehend angemessen und wirksam
- das wesentliche Risiko ist durch IKS-Schlüsselkontrollen reduziert

### Für die Überwachung des IKS empfiehlt sich eine Kombination aus Self Assessment & Control Testing

Optimierung des Prozesses zur Überwachung von Angemessenheit und Wirksamkeit des IKS durch eine Kombination aus zentralen und dezentralen Elementen hat sich im Markt etabliert.



Bei der Ausgestaltung des Überwachungsprozesses sollten folgende Kriterien beachtet werden:

1. Belastbarkeit der Ergebnisse des Überwachungsprozesses
2. Ressourcenaufwand für die Durchführung des Überwachungsprozesses

## Die Schlanke Linie

Stärkung der Zusammenarbeit und Verzahnung der einzelnen Kontrollfunktionen (insb. 2nd Line) hinsichtlich der Überwachung der operativen Einheiten basierend auf einheitlichen Strukturelementen

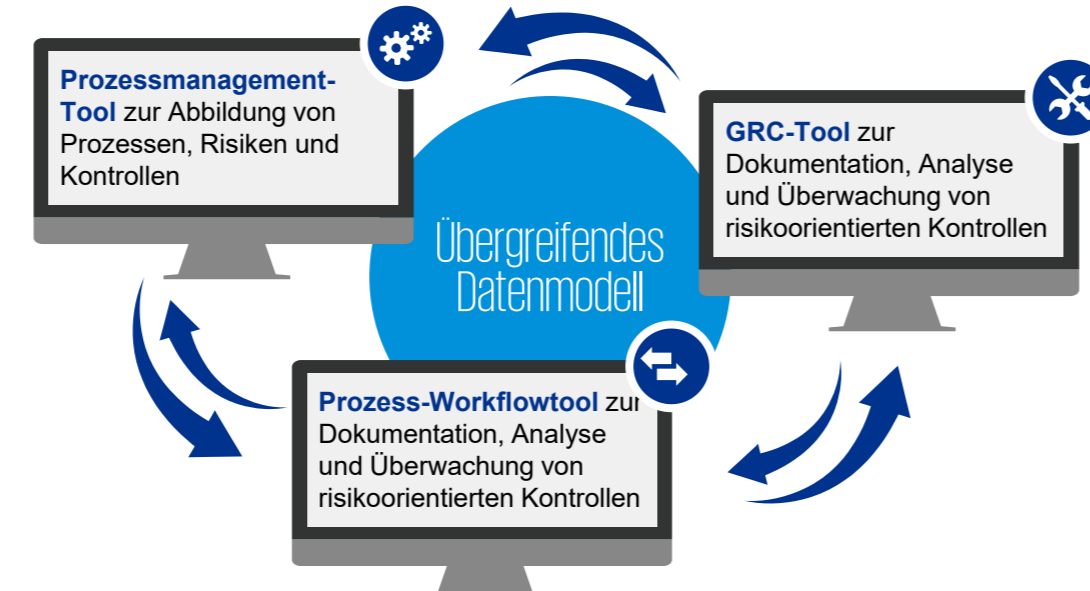


## Ihre Ansprechpartner

- KPMG AG Wirtschaftsprüfungsgesellschaft  
www.kpmg.com/de
- Markus Weddehage**  
T +49 69 9587-3459  
mweddehage@kpmg.com
- Thorsten Janker**  
T +49 69 9587-2596  
tjanker@kpmg.com
- Daniel Ziegler**  
T +49 89 9282-4496  
dziegler@kpmg.com
- Dr. Stephan Braun**  
T +49 69 9587-4617  
stephanbraun@kpmg.com



## Digitalisierung des IKS zur Steigerung von Effizienz und Qualität



### Herausforderung & Zielsetzung

- Konzepte zur Weiterentwicklung des Internen Kontrollsystems insb. im Hinblick auf die Zusammenarbeit und Verzahnung mit anderen 2nd Line-Funktionen sind nur dann effizient operativ umsetzbar, wenn sie systemseitig unterstützt und geleitet werden
- Die eingesetzten Tools und Lösungen benötigen dabei Informationen zu Prozessen, Risiken, Kontrollen und Verantwortlichkeiten
- Zur Vermeidung von Redundanzen und Inkonsistenzen ist daher durch alle Kontrollfunktionen auf eine einheitliche Datengrundlage auf Basis der unternehmensweiten Prozesslandkarte zurückzugreifen (Single Source of Truth) und diese um Erkenntnisse aus den einzelnen Themengebieten (bspw. Wesentlichkeit, Wirksamkeit) anzureichern

### Ansätze zur Digitalisierung des IKS (Auswahl)

- Automatisierung von Kontrollen
- Bewertung von Risiken und Digital Risk Assessment
- Dokumentation der Kontrolldurchführung
- Workflow IKS-Regelkreis
- Continuous Control Monitoring
- Reporting Funktionalitäten und strukturierte Auswertbarkeit der Überwachungsaufgaben

## Ziele und Key-Benefits eines effizienten IKS

- Prozesslandkarte mit unternehmensweit durchgängiger Prozessdokumentation**
  - Transparenz über Tätigkeiten, Beteiligte und Abhängigkeiten entlang der Prozesskette
- Konsistente Definition und prozessbezogene Zuordnung wesentlicher Risiken und Schlüsselkontrollen**
  - Fokussierung auf relevante Handlungsfelder
- Eindeutige Verantwortlichkeiten** durch klares **Rollenverständnis**
  - Kontinuierliche Beschäftigung mit der Kontrollverantwortung sowie Transparenz über deren Verteilung
- Systematischer IKS-Überwachungsprozess**
  - gebündelte Informationen zu IKS-Schwächen
  - „selbst lernendes“ System über die unternehmensweite Prozesslandkarte
- Verzahnung diverser „Kontrollfunktionen“** zur Hebung von Synergien und Sicherstellung einer **gemeinsamen „IKS-Sprache“**
- Prozess- und Kontrolldokumentation** als Grundlage für **Effizienzanalysen**