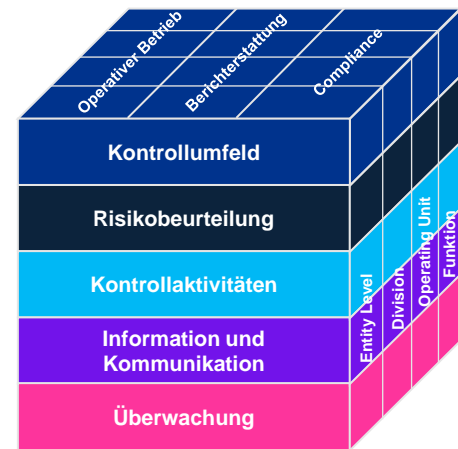




# Effizient, sicher & digital – unsere Ansätze für die Ausgestaltung des Internen Kontrollsystems (IKS) im Financial Services-Umfeld

## Definition des Internen Kontrollsystems



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)

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**)

## Regulatorische Grundlagen

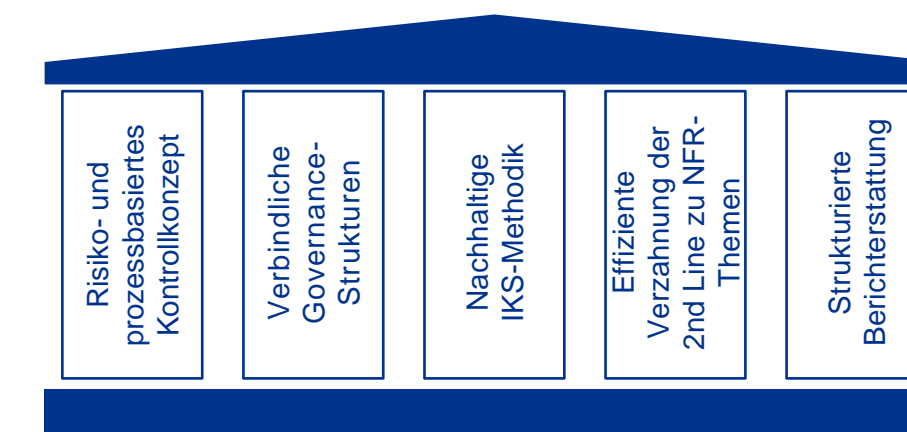


Den übergreifenden Rahmen für das IKS im FS-Umfeld bilden insb.

- § 91 (2) und § 107 (3) AktG
  - die Prüfungsstandards ISA 315, IDW PS 951, IDW PS 982 und ISAE 3402
  - der Deutsche Corporate Governance Kodex
- Daneben existieren verschiedene branchenspezifische Ergänzungen (Auswahl):
- Banken: § 25a 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
  - Zahlungsdienstleister: § 27 ZAG und AT 4.3 ZAG-MaRisk

## Säulen eines strukturierten IKS

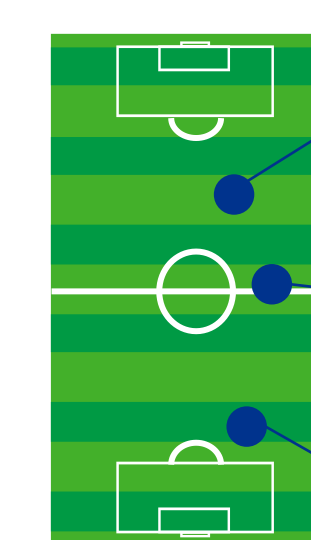
Zur Operationalisierung des unternehmensweiten IKS sind verschiedene Säulen zu berücksichtigen



## IKS@3LoD

Eine Ausrichtung entlang der 3 Lines of Defence dient der Förderung eines systematischen Ansatzes zur Identifikation und Handhabung von Unternehmensrisiken auf drei voneinander unabhängigen Ebenen unterhalb der Unternehmensleitung.

Diese Ausrichtung ist bei der Ausgestaltung, Steuerung und Überwachung des unternehmensweiten IKS von zentraler Bedeutung



**First Line**  
Operative Bereiche (z.B. Markt, Vertrieb)

**Second Line**  
Kontrollfunktionen (z.B. Risikomanagement, Compliance)

**Third Line**  
Interne Revision

Ausgestaltung von Prozessen, Identifikation von Risiken und Einrichtung angemessener und wirksamer Kontrollen

Hinwirkung durch Vorgabe von Anforderungen und Minimum Control Standards sowie Überwachung der 1st Line hinsichtlich der angemessenen und wirksamen Umsetzung dieser

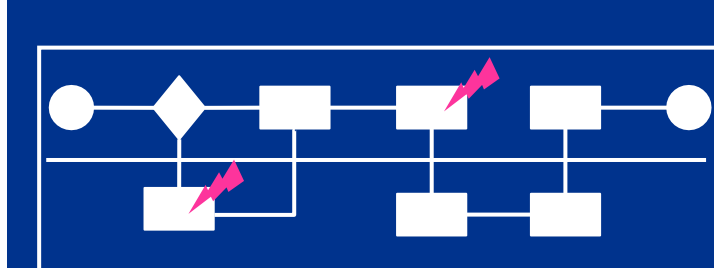
Prozessunabhängige Prüfungsinstanz des IKS über alle Einheiten des Unternehmens hinweg

## 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-to-End-Prozessbetrachtung wird die vollständige, konsistente und redundanzfreie Identifikation nicht-finanzieller Risiken sichergestellt.

#### Kernelemente der Prozess-, Risikoanalyse



Welche **relevanten Prozessschritte** gibt es im Prozess?

- Strukturierung der Prozesse in einem Ebenenmodell
- Einheitliche und konsistente Erfassung der Prozesse

Welches sind die **wesentlichen nicht-finanziellen Risiken** im Prozess?

- Identifikation der „what could go wrongs“ entlang des Prozesses (prozessinhärente Brutto-Risiken)
- Zuordnung der Risiken zu den Risikoarten des Non-Financial Risk Managements

#### Prozess- und Risikoanalyse

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

Basierend auf der Wesentlichkeit der Risiken werden angemessene Kontrollen zugeordnet, um das Risiko hinreichend zu reduzieren

#### Abgrenzung von Kontrollen

Kontrolle: „Jede Aktivität, die dazu dient, Risiken zu steuern (vermeiden, verhindern oder aufdecken) und die Wahrscheinlichkeit zu erhöhen, dass bestehende Prozesse eingehalten und gesetzte Ziele erreicht werden.“

Wesentliches Risiko

Bedeutendes Risiko

Geringes Risiko

Schlüsselkontrolle

Standardkontrolle

Vereinfachte Kontrolle

- Zwingend erforderlich für die deutliche Reduzierung eines **wesentlichen Risikos**
- **Abwesenheit dieser Kontrolle kann zu signifikanten Fehlern** im betroffenen Prozess führen
- Reduzierung eines nicht-wesentlichen, jedoch **bedeutenden Risikos**
- Kann auf die **Reduzierung eines wesentlichen Risikos** einzahlen, bei deren Versagen werden jedoch die Fehler durch Schlüsselkontrollen aufgefangen
- Optionale Kontrolle zur Reduktion von **geringen Risiken**
- Erfassung nur, wenn sie aktiv zur Reduktion der prozessinhärenten Risiken geleistet werden

### Die Überwachung erfolgt als Kombination aus Self Assessment & Control Testing

Die Überwachung von Angemessenheit und Wirksamkeit ist das Kernelement des Regelkreises und in unterschiedlichen Ausprägungen etabliert.

#### Elemente des Überwachungsprozesses

Self Assessment

Kontrollfunktion

Konsolidierung und Plausibilisierung

Prozess-/Kontrollverantwortlicher

Unabhängiges Control Testing

IKS-Instanz

- Strukturierter Prozess zur Ableitung von Angemessenheit und Wirksamkeit sowie nachvollziehbares Reporting ist erforderlich und zudem Marktstandard
- Ausgestaltung von Self Assessment und Control Testing in der Umsetzung sehr heterogen und abhängig vom Zusammenspiel mit anderen Kontrollfunktionen sowie dem Risikoappetit des Unternehmens

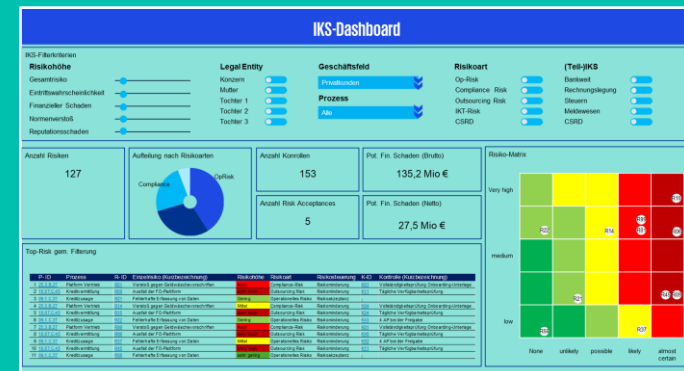
### Das Ergebnis des IKS-Regelkreises ist ein aussagekräftiges Reporting

Angemessenheits- und Wirksamkeitsbestätigung in einem IKS-Reporting, 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
  - Führungskräfte: zur Information über den Zustand des IKS in ihrem Bereich
  - Reporting muss je nach Empfänger unterschiedliches Granularitätsniveau haben

- Zielsetzungen des IKS-Reportings von morgen
- Auswertung unter Berücksichtigung individueller Risikoappetite
  - Integration der „Teil-IKS“ ohne Abstriche bei der erforderlichen Granularität
  - Keine Einschränkung auf wesentliche Risiken
  - Verstärkter Fokus auf die Optimierung der Kontrolllandschaft



## IKS als Regelgeber und Klammer

Das unternehmensweite IKS berücksichtigt die prozessinhärenten Risiken über **alle Non-Financial Risk-Arten** hinweg und umfasst somit Kontrollen unterschiedlicher Anforderungen und Teil-Disziplinen



#### Vorteile einer unternehmensweiten Betrachtung des IKS

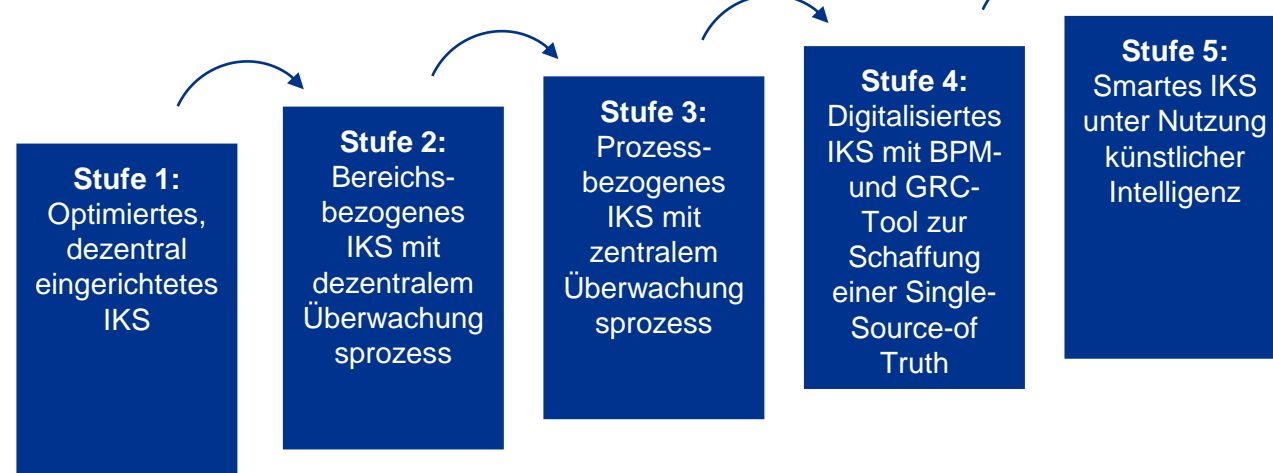
- Regelungsgeber: Einheitliche Konventionen und Strukturierung für alle Risiken und Kontrollen entlang der Prozesse des Hauses
- Klammerfunktion: Umfassendes Risiko- und Kontrollinventar mit Transparenz über Schnittstellen, Abhängigkeiten und Zusammenhänge zwischen einzelnen Risikoarten, Anforderungen und Teil-Disziplinen

#### Wichtige Voraussetzungen für die Abbildung des unternehmensweiten IKS

- Klare Zuordnungen von Risiken und Kontrollen zur jeweils relevanten nicht-finanziellen Risikoart
- Mapping der Kontrollen zu spezifischen Disziplinen zur Ermöglichung spezifischer Auswertung und Steuerung/Überwachung
- Nutzung der vorhandenen IKS-Strukturelemente und -Informationen bei der Adressierung neuer Anforderungen

## Evolutionsstufen des IKS

Das IKS entwickelt sich stetig weiter. Mit Blick auf den Markt lassen sich fünf Stufen ableiten:



## Das Smarte IKS: Digitalisierung und KI zur Steigerung der Effizienz und Qualität

Für die Umsetzung eines smarten IKS sehen wir (mindestens) die folgenden Bausteine

#### Automatisierung und Datenverfügbarkeit

Die Automatisierung von Prozessen und Kontrollen und die Datenverfügbarkeit von IKS-Informationen bilden die Grundlage für alle weiteren Überlegungen

#### IKS Opti 2.0

Eine optimierte Operationalisierung des IKS fördert die Effektivität und Effizienz des IKS und stärkt zugleich den Mehrwert



#### Aktiv compliant

Zur Sicherstellung einer hinreichenden Flexibilität muss das IKS aktiv auf neue und geänderte Rahmenbedingungen reagieren können

#### AI-CS

Der Einsatz von AI im IKS (AI-CS) stellt die wesentlichste Neuerung auf dem Weg zum smarten IKS dar – und erlaubt eine Revolution der Steuerung und Überwachung

#### #Mehrwert@Business

Die Steigerung des Mehrwerts aus einem smarten IKS muss konkrete Zahlen, Daten und Fakten verdeutlicht werden – wichtig ist, dass der Mehrwert sichtbar ist und gesehen wird

## Key-Benefits eines smarten und effizienten IKS



Umfassende Prozessdokumentation mit allen IKS-relevanten Informationen im BPM- und GRC-Tool als **Single Source of Truth** für das gesamte Unternehmen



**Vollständige Transparenz** über das Risiko- und Kontrollinventar durch Erhebung der Risiken entlang des NFR-Katalogs und Zuordnung der relevanten Kontrollen



Eindeutige **Verantwortlichkeiten** durch klares **Rollenverständnis über alle Verteidigungslinien** hinweg



**Nutzung vorhandener Daten** zur kontinuierlichen Sicherstellung der Compliance, Effektivität und Effizienz von Prozessen und Kontrollen



**Konsistente Aussage zur Angemessenheit und Wirksamkeit des IKS** durch Synchronisation der Ergebnisse diverser „Kontrollfunktionen“ durch einheitliche Strukturen und Methoden basierend auf einer gemeinsamen „IKS-Sprache“



Prozess- und Kontrolldokumentation als Grundlage für **Effizienzanalysen und Optimierungsvorhaben**

## Ihre Ansprechpartner

KPMG AG  
Wirtschaftsprüfungsgesellschaft  
Financial Services Assurance Services

[www.kpmg.com/de](http://www.kpmg.com/de)

**Markus Weddehage**  
Partner Financial Services  
T +49 69 9587-3459  
[mweddehage@kpmg.com](mailto:mweddehage@kpmg.com)



**Dr. Stephan Braun**  
Director Financial Services  
T +49 69 9587-4617  
[stephanbraun@kpmg.com](mailto:stephanbraun@kpmg.com)

