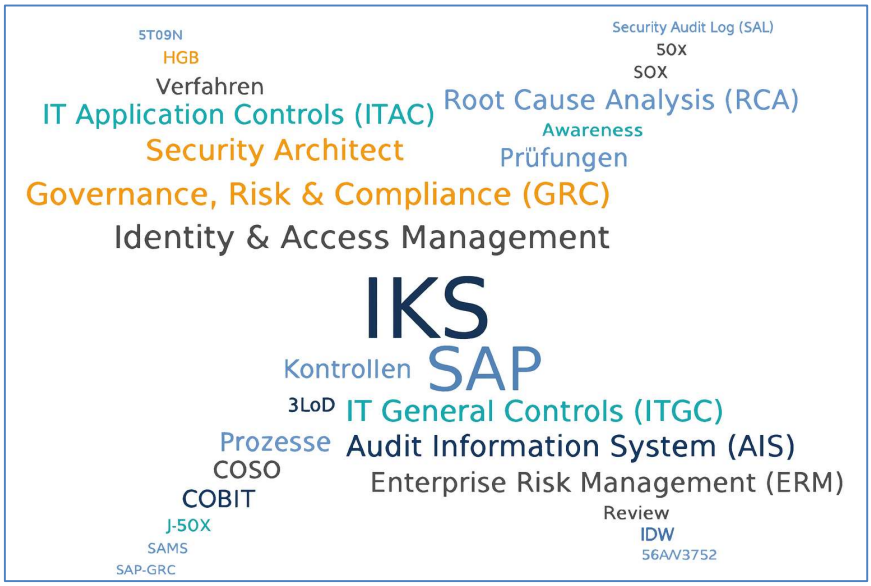
IKS für SAP-Systeme – gesetzlich gefordert, praxisnah umsetzbar

Effiziente Einführung, revisionssichere Dokumentation, gezielte SAP-Kontrollen



Ein **Internes Kontrollsystem (IKS)** ist für Kapitalgesellschaften nicht nur ein rechtliches Muss, sondern ein zentrales Instrument, um Risiken zu steuern, Prozesse zu sichern und die Unternehmensführung zu stärken.

Die **gesetzliche Grundlage** ist eindeutig: Geschäftsführung und Vorstand tragen die volle Verantwortung für die Existenz, Wirksamkeit und Dokumentation eines IKS. Im Prüfungsfall kann eine unzureichende Umsetzung erhebliche Konsequenzen haben – sowohl organisatorisch als auch persönlich.

Doch ein IKS ist weit mehr als eine Pflichtübung: Richtig konzipiert und umgesetzt, wird es zu einem wirkungsvollen **Werkzeug für Transparenz, Sicherheit und Effizienz**. Es schafft Klarheit über Rollen und Zuständigkeiten, zeigt sinnvolle Kontrollen und Prüfungen, reduziert Prüfungsstress und liefert belastbare Nachweise gegenüber dem Management, interner Revision, Wirtschaftsprüfern und Aufsichtsbehörden.

Ihre Vorteile auf einen Blick

- Revisionssichere Dokumentation
- Strukturierte Kontrollen und Prüfungen
- Gezielte SAP-Integration
- Klare Verantwortlichkeiten und Rollen
- Mehr Sicherheit und weniger Prüfungsstress

Im Folgenden erfahren Sie, welche gesetzlichen Grundlagen für Sie relevant sind, wie ein IKS mit SAP-Praxisbezug aufgebaut wird und welche Tools Sie dabei wirksam unterstützen.

Gesetzliche Anforderungen & IKS-Pflichten

Ein wirksames Internes Kontrollsystem (IKS) ist nicht nur eine gesetzliche Pflicht, sondern ein zentrales Führungsinstrument. Die Geschäftsführung ist für die Einrichtung, Dokumentation und Überwachung verantwortlich – unabhängig von der Unternehmensgröße. Im Prüfungsfall muss die Wirksamkeit nachgewiesen werden können.

Gesetzliche Basis (Auswahl):

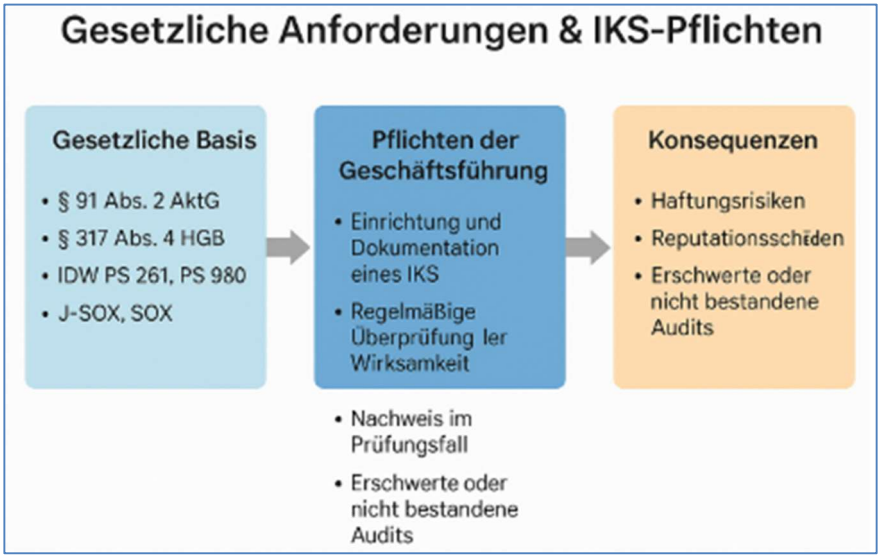
- § 91 Abs. 2 AktG – Risikofrüherkennung
- § 317 Abs. 4 HGB – Prüfung des internen Kontroll- und Risikomanagementsystems
- IDW PS 261, PS 980 – Prüfungsstandards
- SOX, J-SOX – internationale Parallelen

Pflichten der Geschäftsführung:

- Einrichtung und Dokumentation eines IKS
- Regelmäßige Überprüfung der Wirksamkeit
- Nachweis im Prüfungsfall

Konsequenzen bei Pflichtverletzung:

- Haftungsrisiken
- Reputationsschäden
- Erschwerte oder nicht bestandene Audits



Vorgehensmodell zur IKS-Einführung

Die erfolgreiche Einführung eines Internen Kontrollsystems (IKS) im SAP-Umfeld erfordert ein strukturiertes Vorgehen. Ein bewährtes Modell besteht aus vier klar definierten Phasen, die den gesamten Lebenszyklus eines IKS abdecken – von der Analyse über die Konzeption und Umsetzung bis hin zum laufenden Betrieb und der kontinuierlichen Verbesserung.

1. Analyse

In dieser Phase werden bestehende Prozesse, Systeme, Kontrollen und Risiken erfasst. Ziel ist es, den Ist-Zustand vollständig zu dokumentieren und erste Schwachstellen zu identifizieren. Dies umfasst sowohl technische SAP-Parameter als auch organisatorische Abläufe.

2. Konzept

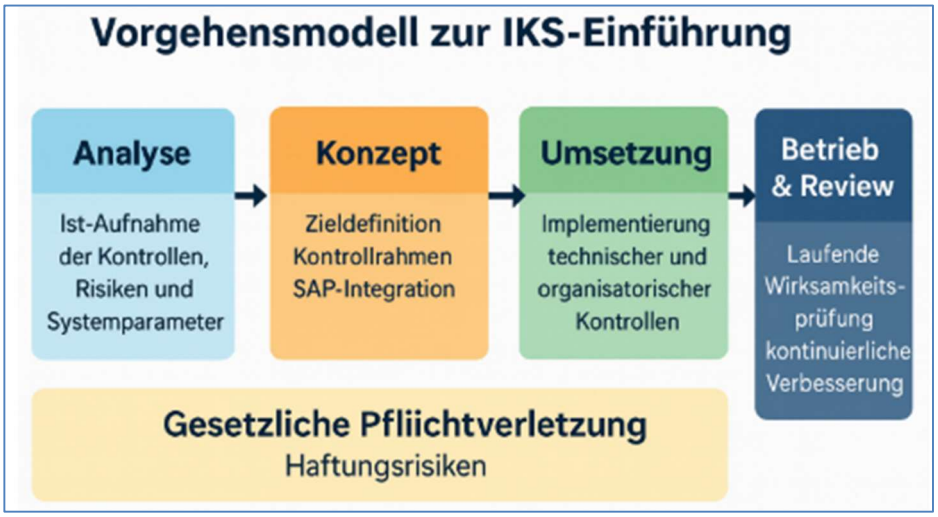
Basierend auf den Ergebnissen der Analyse werden Ziele, Kontrollrahmen und Integrationspunkte in SAP definiert. Dazu gehören die Festlegung von Verantwortlichkeiten, die Auswahl geeigneter Kontrollen und die Planung der erforderlichen technischen sowie organisatorischen Maßnahmen.

3. Umsetzung

In dieser Phase werden die im Konzept definierten Maßnahmen implementiert. Dies beinhaltet die technische Umsetzung in SAP (z. B. Berechtigungen, Protokollierungen, Automatisierungen) sowie die Einführung organisatorischer Kontrollen wie Checklisten, Vier-Augen-Prinzip oder Freigabeprozesse.

4. Betrieb & Review

Nach der Umsetzung beginnt der laufende Betrieb des IKS. Die Wirksamkeit der Kontrollen wird regelmäßig überprüft, und das System wird fortlaufend an neue gesetzliche Anforderungen, organisatorische Veränderungen und technische Entwicklungen angepasst. Ziel ist die kontinuierliche Verbesserung.



Checkliste zur IKS-Reife im SAP-System

Diese Checkliste bietet einen kompakten Überblick zur Bewertung der IKS-Reife im SAP-System. Sie eignet sich für einen Selbst-Check oder als Grundlage für interne Audits.

Bitte beachten: Es handelt sich hier nur um einen Auszug aus einer deutlich umfangreicheren Checkliste.

Prüf-Frage	**Status**	**Anm.**
Kritische SAP-Systemparameter dokumentiert?	🟢 / 🟡 / 🔴	
SoD-Konflikte analysiert und reduziert?	🟢 / 🟡 / 🔴	
Relevante SAP-Logs aktiviert und ausgewertet?	🟢 / 🟡 / 🔴	
Verantwortlichkeiten für Kontrollen klar definiert?	🟢 / 🟡 / 🔴	
Notfallbenutzer-Nutzung dokumentiert und geprüft?	🟢 / 🟡 / 🔴	
Änderungen an Berechtigungen nachvollziehbar?	🟢 / 🟡 / 🔴	
IKS-Dokumentation vollständig und aktuell?	🟢 / 🟡 / 🔴	
Review- und Verbesserungsprozess etabliert?	🟢 / 🟡 / 🔴	
Backup- und Wiederherstellungsprozesse regelmäßig getestet?	🟢 / 🟡 / 🔴	
SAP-Transportmanagement revisionssicher dokumentiert?	🟢 / 🟡 / 🔴	
Benutzer mit erweiterten Rechten regelmäßig überprüft?	🟢 / 🟡 / 🔴	
IKS-Trainings für relevante Mitarbeiter durchgeführt?	🟢 / 🟡 / 🔴	

Hinweis: Diese Liste ist ein Auszug – die vollständige Checkliste umfasst deutlich mehr Prüfpunkte.

Legende: 🟢 **= erfüllt,** 🟡 **= teilweise erfüllt,** 🔴 **= nicht erfüllt**

SAP-Funktionen & Tools mit IKS-Relevanz

Eine wirksame IKS-Umsetzung im SAP-Umfeld hängt maßgeblich von der Nutzung der richtigen Analyse- und Kontrollfunktionen ab. Die folgenden Tools sind im SAP-Standard enthalten und stellen zentrale Bausteine für Prüfung, Optimierung und Sicherheit dar.

Tool / Funktion	IKS-Nutzen & Beschreibung	Typische Einsatzbeispiele
Audit Information System (AIS)	Lizenzfrei im SAP-Standard, liefert vordefinierte und eigene Auswertungen zu kritischen Prozessen. Ideal zur Unterstützung von internen und externen Audits.	Kontrolle kritischer Benutzer Prüfen von Änderungsprotokollen Analyse von Belegänderungen
Security Audit Log (SAL)	Protokolliert sicherheitsrelevante Aktivitäten wie An- und Abmeldungen, Berechtigungsänderungen oder RFC-Aufrufe. Unverzichtbar für forensische Analysen.	Überwachung kritischer Transaktionen Nachweis bei Sicherheitsvorfällen
ST03N – Workload-Analyse	Zeigt detaillierte Nutzungsmuster, Antwortzeiten und Auslastung. Hilft, ungewöhnliche Aktivitäten zu erkennen.	Erkennen ungenutzter Rollen/Berechtigungen Analyse von Performance-Engpässen
SU24 / SU25	Unterstützt die saubere Pflege der Berechtigungsprüfungen und Rollenpflege, reduziert SoD-Konflikte und manuelle Nacharbeiten.	Rollendesign optimieren Pflege der Vorschlagswerte
Systemparameter-Prüfung	Überprüft und bewertet sicherheitsrelevante SAP-Parameter gegen Best-Practice- und Audit-Vorgaben.	Parameter „login/min_password_lng“ prüfen RFC-Sicherheitsparameter kontrollieren

Weitere SAP-Kontrollen im ITGC-Kontext:

(1) Identity & Access Management (IAM)

Nr	SAP-Element	Beschreibung / Verwendungszweck
1	SU01 / SU10	Benutzerpflege (Einzel / Massenerstellung)
2	PFCG	Rollenerstellung, Berechtigungszuweisung
3	SUIM (div.)	Reports zur Berechtigungsvergabe, Rollenzuordnung, Benutzergruppen
4	ST03N	Nutzungsauswertung je Benutzer / Transaktion
5	STAD / ST01	Einzelfall-Analyse zu Benutzeraktionen (z. B. Protokoll von kritischen Aktionen)
6	RSUSR200	Prüfung von Benutzern mit kritischen Rechten
7	RSUSR003	Passwort-Status, Gültigkeit, Passwortregeln
8	SU24 / SU25	Pflege von Berechtigungsvorschlägen

SAP-Elemente für IAM-Kontrollen

(2) Programmentwicklung und Transportwesen

(3) IT-Betrieb und Infrastruktur (Operations)

(4) Systemintegrität und Schnittstellen

Praxisbeispiel & Originalpassagen (IAM)

Originalpassage (Kapitel 9.3.1.1 – Identity & Access Management):

„Identity & Access Management“ (IAM) umfasst sämtliche Prozesse, Richtlinien und Systeme zur Verwaltung von digitalen Identitäten und zur Steuerung des Zugriffs auf IT-Systeme, Anwendungen und Daten. IAM stellt sicher, dass nur berechtigte Personen unter kontrollierten Bedingungen Zugang zu Informationen und Ressourcen erhalten – und zwar nach dem Prinzip der minimalen Rechtevergabe („Least Privilege“).

Originalpassage (Kapitel 11.5.1 – IAM: Bewertung):

SAP bietet im IAM-Bereich eine große Anzahl an standardisierten, aber auch ergänzbar programmierbaren Kontrollen. Besonders relevant ist das Thema SoD (Segregation of Duties):

- Mit SUIM und Z-Reports lassen sich funktionale Inkompatibilitäten identifizieren.
- Eine strukturierte SoD-Matrix (vgl. Kapitel 12.4.4) ermöglicht systematische Risikoanalysen.
- Ohne SAP-GRC-Tool erfordert dies jedoch ein hohes Maß an manueller Analysekompetenz.

Originalpassage (Kapitel 11.4.4 – Periodische oder Event-getriebene Prüfhandlungen):

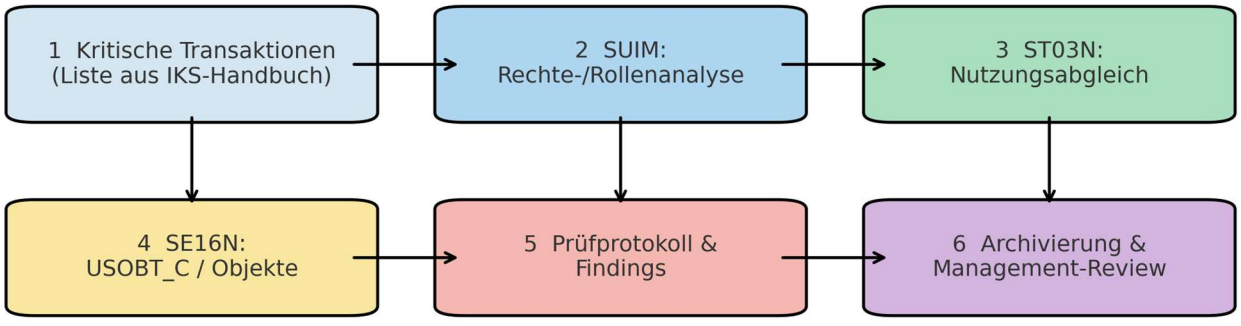
Viele SAP-Kontrollen werden nicht ständig, sondern z. B. monatlich oder ad-hoc durchgeführt,

- RSUSR002 / RSUSR003: Prüfung von Benutzerstammdaten
- Z-Berichte zur Belegprüfung oder kritischen Transaktionen
- Berechtigungsreviews mit Excel-Export und Sign-off

Praxisbeispiel – Regelmäßige Berechtigungsprüfung im SAP-System (IAM):

Kontrolle:	Auswertung kritischer Transaktionen und Berechtigungen
Prüfziel:	Sicherstellen, dass nur berechtigte Personen Zugriff auf sensible Transaktionen haben
Prüfmethode:	SUIM (Rollen-/Berechtigungsprüfung), ST03N (Nutzungsanalyse), SE16N (USOBT_C/Obj.)
Frequenz:	Monatlich bzw. gemäß Kap. 11.4.4
Nachweis:	Prüfprotokoll im IKS-Handbuch; revisionssichere elektronische Ablage
Hinweis:	Details zu SAP-Elementen siehe IKS-Handbuch Kap. 11.5.1 (Tabelle 11-3) und Tabelle auf Seite 5 dieser Broschüre.

Ablaufdiagramm – Berechtigungsprüfung (Flowchart):



Inhaltsverzeichnis des IKS-Handbuchs

Im Folgenden die Gliederung und das Inhaltsverzeichnis der Version 1.0 des aktuellen IKS-Handbuchs. Insgesamt hat das IKS-Handbuch 272 Seiten mit 29 Abbildungen und 41 Tabellen.

Mit diesem Anhang erhalten Sie einen kompakten, praxisnahen Überblick, der den Weg von der Theorie zur Umsetzung in fünf klaren Phasen strukturiert und so den Einstieg in das IKS-Handbuch erleichtert.