

Klassifikations- und Dokumentationsmodell des IKS

Definition IKS: Das Interne Kontrollsystem (IKS) ist das zentrale Management-Werkzeug der unternehmensinternen betriebswirtschaftlichen Überwachung. Dieses Werkzeug wird auf Kontroll-Objekte des Unternehmens angewandt; hierbei werden Kontroll-Ziele der IKS-Zielfelder verfolgt. Das IKS wird selbst zu einem Kontroll-Objekt erklärt.

Zielfelder des IKS	
ZK1 Rechtskonformität	Einhaltung der rechtlichen Vorschriften
ZK2 Strategie-Adhärenz	Einhaltung der definierten Geschäftsstrategie
ZK3 Bilanz-Qualität	Ordnungsmäßigkeit der Rechnungslegung
ZK4 Prozess-Qualität	Sicherheit, Effizienz, Wirksamkeit der Prozesse
ZK5 Asset-Schutz	Schutz: Güter, Vermögen, Daten & Informationen

Instrumente: Die Umsetzung der Resultate von Analysen des IKS erfolgt in Form von Kontrollen, Vorkehrungen, Beauftragungen etc; das umgesetzte Einzel-Resultat wird als Instrument bezeichnet und einer der folgenden IKS-Instrument-Klassen zugeordnet und die Art des Instruments durch einen Typ näher gekennzeichnet:

Kontroll-Objekte des IKS	
Governance - Gestaltung	
IKS (IKi/OFi) (i=1-5)	
Organisation (Gestalt)	
Grundsatz – Einrichtung – Verfahren - Maßnahme	
Ereignisse – (Ablauf-Gestalt)	
Organisation (Ablauf)	
IT-Prozess	
IT-Ereignis	
Geschäftsprozess	
Geschäftsvorfall	
int. Leistungsprozess	
Ressourcen – (Aufbau-Gestalt)	
IT-Verbund (allgemein)	
Raum - IT-System	
IT-Link - IT-Anwendung	
Organisation (Aufbau)	
Abteilung – Rolle - Person	
Daten-Objekte	
Stammdaten -Belege –	
Dokumente - Konten	
Journale - Protokolle	

IK1 Grundsätze	Policies, Richtlinien;	Vorkehrung
IK2 Organisation	Aufbau: Organisationsplan	Kontrolle, Vorkehrung
IK3 Einrichtungen	Installierte technische Elemente	Kontrolle, Vorkehrung, Prüfung
IK4 Verfahren	Prozess: Gestalt, Anweisungen	Kontrolle, Vorkehrung, Prüfung
IK5 Maßnahmen	Management-Gestaltungseingriff	Kontrolle, Vorkehrung, Beauftragung, Revision

Komponenten: Die Aktivitäten des IKS erfolgen in Operationsfeldern (Komponenten n. IDW, COSO):

OF1 Kontrollumfeld	Einstellungen, Problembewusstsein, Unternehmenskultur
OF2 Risikoerkennung	Erkennung und Analyse von Unternehmensrisiken
OF3 Kontrollaktivitäten	Kontrollen (integriert, intellektuell), IKS-Kalender
OF4 Information/ Kommunikation	Richtlinien, Handbücher, Berichte
O5 Überwachung des IKS	Beurteilung der Wirksamkeit des IKS

Ende Definition IKS

Dokumentationsmodell

Bausteine: Das auf ein konkretes Kontroll-Objekt angewandte Werkzeug heißt Baustein¹; es stellt eine Fragestellung dar. Die Fragestellung verfolgt ein Kontrollziel aus einem Zielfeld $z_f \in \{ZF1..ZF5\}$ und klassifiziert den Baustein Die Bearbeitung (Analyse/Untersuchung) liefert eine Resultatmenge:

Baustein => **KOB** => {**Resultat**(IK_i)}; ($i \in 1..5$)

Jedes Resultat der Resultatmenge lässt sich einer Instrumentklasse zuordnen. $R_j \Rightarrow \{IK1..IK5\}$.

Der Baustein wird durch einen Bezeichnung, eine Fragestellung, ein Kontroll-Objekt, einem Kontrollziel und einem entsprechenden Klassenbezeichner aus den Zielfeldern ZF bestimmt.

Projekte und Anwendungen: In der Zeitspanne von der Initiierung bis zum Resultat werden alle Tätigkeiten und Dokumente, die bei der Bearbeitung des Bausteins manifest werden, als **IKS-Projekt** bezeichnet. Das Projekt wird als **Dokumentations-Objekt** repräsentiert. Ein implementiertes Resultat heißt **IKS-Anwendung**. Objekte des Berichtswesens und andere Informationen (auch mündliche) werden als **Bericht** bezeichnet. Das Ergebnis der Analyse eines Berichts heißt **Auswertung**.

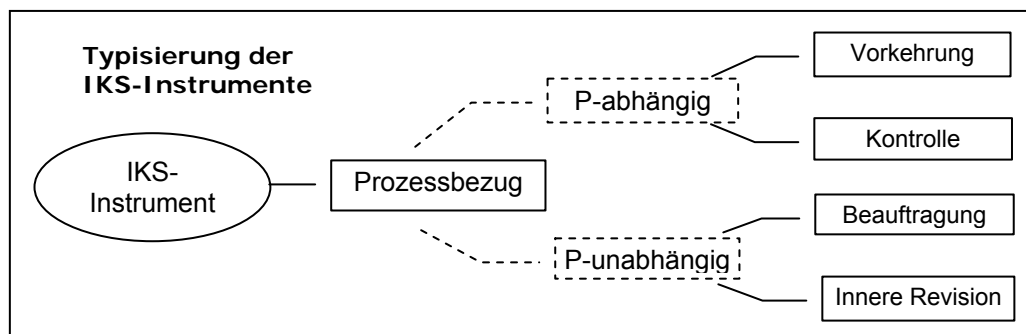
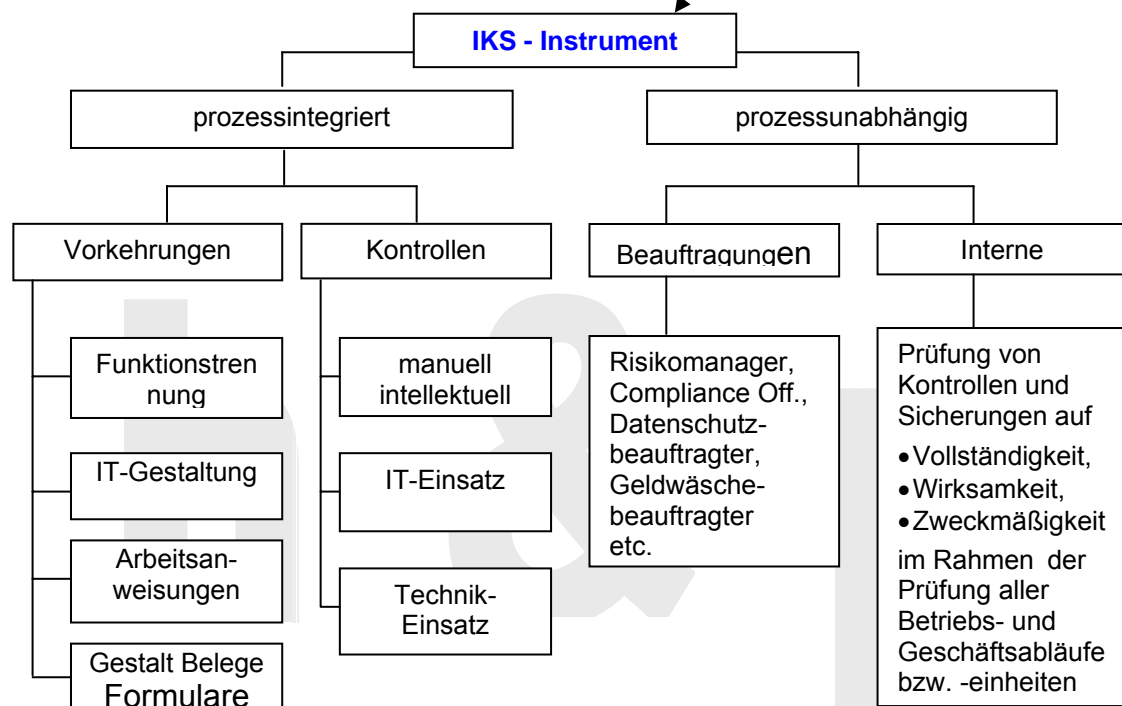
IKS-Kalender: Im IKS-Kalender werden **Projekte**, **Anwendungen** und **Berichte** sowie freie, nicht näher klassifizierte Termine für **Kontroll-Objekte** und **Kontroll-Aktivitäten** geführt

Ende Dokumentationsmodell

¹ **Anmerkung:** Baustein wird hier gewählt, um in der Bezeichnungsweise analog zur Terminologie des BSI beim GSHB zu bleiben.

Einordnung und Typisierung der IKS-Instrumente

IKS-Komponente	IKS-Zielfeld				
	Rechtskonformität	Strategie-Adhärenz	Bilanz-Qualität	Prozess-Qualität	Asset-Schutz
Kontrollumfeld					
Risikomanagement					
Kontrollaktivitäten	IKS-Instrumente²				
Information/Kommunikation					
Überwachung des IKS					



Sprachgebrauch

Es werden folgende Attribute für IKS-Ereignisse verwendet:

- **manuell**
- **interaktiv**
- **vorkehrend**
- **Int. Revision**
- **automatisch**
- **kontrollierend**
- **auswertend**

² Quelle dieses Diagramms und der Systemischen Kontrollen s.u.: Deutscher Sparkassenverband

Vorkehrungen	
	Kontrollziele allgemein <ol style="list-style-type: none"> 1. Fehler verhindern 2. Sicherheitsniveau gewährleisten
	Funktionstrennung³ <ol style="list-style-type: none"> 1. Die Funktionstrennung auf Abteilungsebene. (ORG-Aufbau) 2. Die Funktionstrennung beim Geschäftsvorfall (Org-Ablauf)
	Sicherungsmaßnahmen per IT- und Org-Aufbau (Gestalt) <ol style="list-style-type: none"> 1. Gestaltung von Geschäftsvorfällen 2. Zugriffsberechtigungen/-beschränkungen 3. Datenschutzmaßnahmen 4. Arbeitsanweisungen Dateneingabe 5. Eingabekontrollen (before the act) 6. Behandlung fehlerhafter Eingaben 7. Systemrichtlinien für IT-Enabling
	Arbeitsanweisungen <ol style="list-style-type: none"> 1. Präzise Regeln (Arbeitsanweisungen) zur Durchführung von Geschäftsvorfällen 2. Klar formulierte Kontrollmechanismen
	Belegwesen und GUIs <ol style="list-style-type: none"> 1. Ergonomischer Aufbau 2. Erkennungssicher
	Kontrollziele des Belegwesens <ol style="list-style-type: none"> 1. identische Bearbeitung gleichartiger Geschäftsvorfälle 2. vollständige und sichere Erfassung von Daten im Rechnungswesen. 3.
	Organisation <ol style="list-style-type: none"> 1. Vorgaben zur Beleg-Gestaltung 2. Steuerung des Belegflusses 3. Sicherung der Belegablage
Kontrollen	
	Kontrollbedarf besteht für Geschäftsvorfälle mit dem Risiko von <ol style="list-style-type: none"> 1. Vermögens-, Informations- oder Wertverlusten 2. nach außen wirkenden Fehlern Kontrollen können in dem zu kontrollierenden Geschäftsvorfall integriert bzw. vor- oder nachgeschaltet sein. Sie können erfolgen durch <ol style="list-style-type: none"> 1. prozessbeteiligte Personen 2. als integrierte IT-Funktion (z.B. Plausibilitätsprüfungen) 3. Stichproben- und/oder nachgelagerte Kontrollen.
	Kontrolle durch Personen intellektuelle Prüfung von Ergebnissen
	Kontrolle durch IT-Instrumente <ol style="list-style-type: none"> 1. autonom automatisch (ohne Interaktion mit Akteuren) 2. prozessintegriert (mit Interaktion mit Akteuren) <p>Die prozessintegrierte Kontrolle soll Fehler möglichst vor Beendigung des Prozesses aufdecken bzw. vermeiden. Diese Art der Kontrolle ist der Nachgelagerten vorzuziehen.</p>
	Kontrolle durch technische Einrichtungen Zugang Gebäude, Räume etc.
Innere Revision	

³ IT-Enabling, Ausführung und Kontrolle eines Geschäftsvorfalles sollen nicht durch ein und dieselbe Person erfolgen (**IT-Enabling** versetzt Mitarbeiter in die Lage IT-gestützte Geschäftsvorfälle durchzuführen).

Systemische Kontrollen					Intellektuell
Prüfmedium	Vollständigkeit	Plausibilität	Konsistenz	Autorisierung	Richtigkeit
Protokollierung	Betragsabstimmung	Format	Kontrollbuchstaben	Identität	Freigabe (Bildschirm)
Verschlüsselung	Postenabstimmung	Grenzwert	Prüfziffern	Berechtigung	Ergebniskontrolle Datenänderung
Biometrisch	Mussfelder	Kombination Datenfelder	Prüfprogramm	Vollmacht	Ergebniskontrolle Eingabe
Chip-Karte		Bestandsabgleich			Fehlerlisten-Bearbeitung
		Existenzprüfung			Belegkontrolle
					Buchungskontrolle

h & p