

## 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	
<b>ZK1 Rechtskonformität</b>	Einhaltung der rechtlichen Vorschriften
<b>ZK2 Strategie-Adhärenz</b>	Einhaltung der definierten Geschäftsstrategie
<b>ZK3 Bilanz-Qualität</b>	Ordnungsmäßigkeit der Rechnungslegung
<b>ZK4 Prozess-Qualität</b>	Sicherheit, Effizienz, Wirksamkeit der Prozesse
<b>ZK5 Asset-Schutz</b>	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:

<b>Kontroll-Objekte des IKS</b>	
<b>Governance</b> - Gestaltung	
IKS (IKi/OFi) (i=1-5) Organisation (Gestalt) Grundsatz – Einrichtung – Verfahren - Maßnahme	
<b>Ereignisse</b> – (Ablauf-Gestalt)	
Organisation (Ablauf) IT-Prozess IT-Ereignis Geschäftsprozess Geschäftsvorfall int. Leistungsprozess	
<b>Ressourcen</b> – (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	

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

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

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

**Ende Definition IKS**

## Dokumentationsmodell

**Bausteine:** Das auf ein konkretes Kontroll-Objekt angewandte Werkzeug heißt Baustein<sup>1</sup>; 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  $\Rightarrow$  KOB  $\Rightarrow$  {Resultat(IK<sub>i</sub>)}; (i  $\in$  1..5)**

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

Der Baustein wird durch eine 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

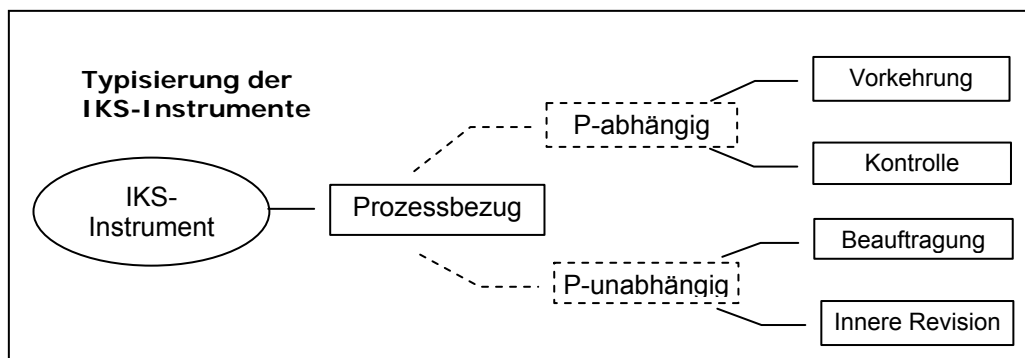
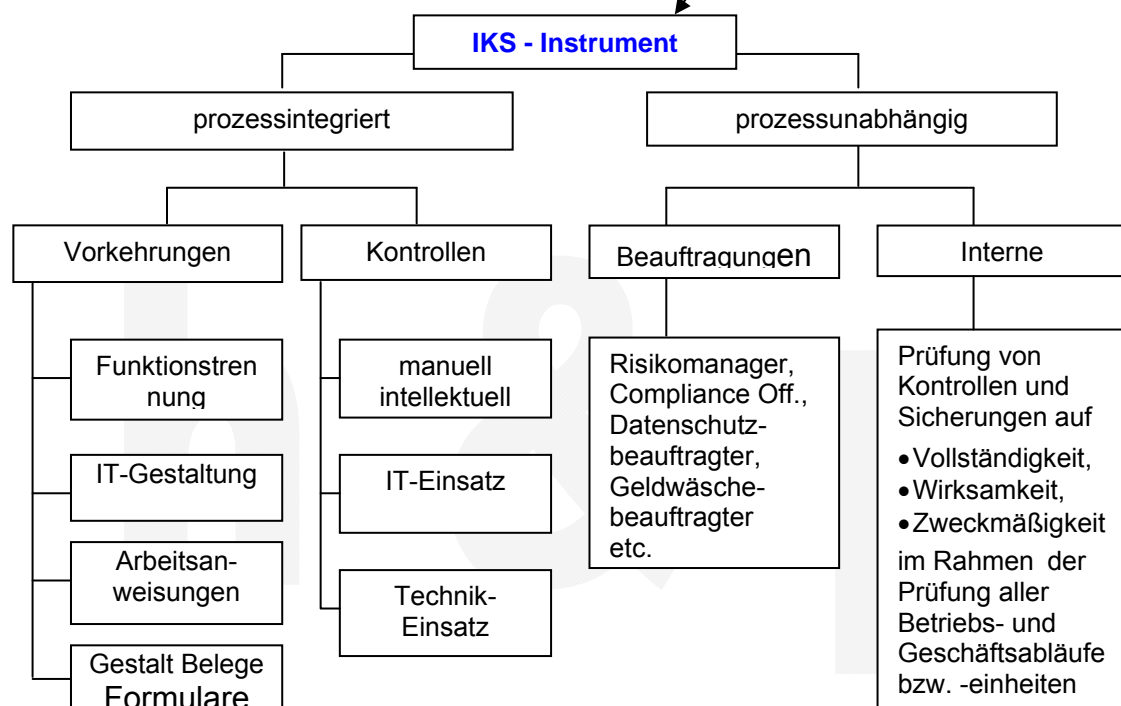
**Ende Dokumentationsmodell**

---

<sup>1</sup> **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	<b>IKS-Instrumente<sup>2</sup></b>				
Information/Kommunikation					
Überwachung des IKS					



<sup>2</sup> Quelle dieses Diagramms und der Systemischen Kontrollen s.u.: Deutscher Sparkassenverband

## Sprachgebrauch

Es werden folgende Attribute für IKS-Ereignisse verwendet:

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

<b>Vorkehrungen</b>	
	<p><b>Kontrollziele allgemein</b></p> <ol style="list-style-type: none"> <li>1. Fehler verhindern</li> <li>2. Sicherheitsniveau gewährleisten</li> </ol>
	<p><b>Funktionstrennung<sup>3</sup></b></p> <ol style="list-style-type: none"> <li>1. Die Funktionstrennung auf Abteilungsebene. (ORG-Aufbau)</li> <li>2. Die Funktionstrennung beim Geschäftsvorfall (Org-Ablauf)</li> </ol>
	<p><b>Sicherungsmaßnahmen per IT- und Org-Aufbau (Gestalt)</b></p> <ol style="list-style-type: none"> <li>1. Gestaltung von Geschäftsvorfällen</li> <li>2. Zugriffsberechtigungen/-beschränkungen</li> <li>3. Datenschutzmaßnahmen</li> <li>4. Arbeitsanweisungen Dateneingabe</li> <li>5. Eingabekontrollen (before the act)</li> <li>6. Behandlung fehlerhafter Eingaben</li> <li>7. Systemrichtlinien für IT-Enabling</li> </ol>
	<p><b>Arbeitsanweisungen</b></p> <ol style="list-style-type: none"> <li>1. Präzise Regeln (Arbeitsanweisungen) zur Durchführung von Geschäftsvorfällen</li> <li>2. Klar formulierte Kontrollmechanismen</li> </ol>
	<p><b>Belegwesen und GUIs</b></p> <ol style="list-style-type: none"> <li>1. Ergonomischer Aufbau</li> <li>2. Erkennungssicher</li> </ol>
	<p><b>Kontrollziele des Belegwesens</b></p> <ol style="list-style-type: none"> <li>1. identische Bearbeitung gleichartiger Geschäftsvorfälle</li> <li>2. vollständige und sichere Erfassung von Daten im Rechnungswesen.</li> <li>3.</li> </ol>
	<p><b>Organisation</b></p> <ol style="list-style-type: none"> <li>1. Vorgaben zur Beleg-Gestaltung</li> <li>2. Steuerung des Belegflusses</li> <li>3. Sicherung der Belegablage</li> </ol>
<b>Kontrollen</b>	
	<p>Kontrollbedarf besteht für Geschäftsvorfälle mit dem Risiko von</p> <ol style="list-style-type: none"> <li>1. Vermögens-, Informations- oder Wertverlusten</li> <li>2. nach außen wirkenden Fehlern</li> </ol> <p>Kontrollen können in dem zu kontrollierenden Geschäftsvorfall integriert bzw. vor- oder nachgeschaltet sein. Sie können erfolgen durch</p> <ol style="list-style-type: none"> <li>1. prozessbeteiligte Personen</li> <li>2. als integrierte IT-Funktion (z.B. Plausibilitätsprüfungen)</li> <li>3. Stichproben- und/oder nachgelagerte Kontrollen.</li> </ol>

<sup>3</sup> 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).

	<b>Kontrolle durch Personen</b> intellektuelle Prüfung von Ergebnissen
	<b>Kontrolle durch IT-Instrumente</b> 1. autonom automatisch (ohne Interaktion mit Akteuren) 2. prozessintegriert (mit Interaktion mit Akteuren)  Die prozessintegrierte Kontrolle soll Fehler möglichst vor Beendigung des Prozesses aufdecken bzw. vermeiden. Diese Art der Kontrolle ist der Nachgelagerten vorzuziehen.
	<b>Kontrolle durch technische Einrichtungen</b> Zugang Gebäude, Räume etc.
<b>Innere Revision</b>	

h & p

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