Modell für die Verfahrensdokumentation nach GoBS IV

Siegfried Mack

Verfahrenswelt
c) Governance
b) Ereignisse
a) Ressourcen

Governance: In den bisherigen Aufsätzen wurde eine Einteilung der Verfahrenswelt in drei Ebenen entwickelt: a) Ressourcen, die aus einer Momentaufnahme heraus erfasst werden konnten, b) wahrnehmbare Ereignisse, die das kaufmännische und TI-Geschehen beschreiben und schließlich die Ebene der Governance, die in der vorliegenden Fortsetzung weiter modelliert werden soll.
Für die Ebenen a) und b) wurden bereits passende Dokumentations-Objekte entwickelt. Jedes Dokumentations-Objekt soll Objekte der Realität zum Verständnis für einen Dritten nachbilden und Veränderungen über der Zeit mitführen.
Bei einem Blick auf die unten stehende Tabelle der bisher gewonnen Objekte fällt auf, dass die Dokumentations-Objekte entweder konkrete Objekte nachbilden (z.B. ein IT-System XXX) oder Klassen von Objekten (z.B. Belege, Geschäftsvorfälle), die die Struktur aller Instanzen beschreiben. Das erklärt auch, weshalb z.B. bei der Darstellung des Geschäftsvorfalles (einer Klasse), der Akteur durch eine Rolle repräsentiert wird und nicht durch den Namen einer konkreten Person. Entsprechend erscheint im Dokumentations-Objekt zur Darstellung des Journals ein Verweis auf den Akteur durch die Angabe „Name" oder „Identifikation-Mitarbeiter". Auf diese Unterscheidung wird auch bei der Modellierung der Ebene der Governance zu achten sein.

Dokumentations-Objekte			
Ressourcen			D-Objekt
	IT-Verbund		
		Container (Gebäude|Raum|Schrank)	real
		Systeme	real
		Infrastruktur (Netzwerk)	real
		Anwendungen	real
	Organisation		
		Abteilungen	real
		Rollen	real
		Personen	real*
	Daten-Objekte		
		Stammdaten	Klasse
		Dokumente	Klasse
		Belege	Klasse
		Konten	Klasse
		Journale	Klasse
	Datenträger	Datenträger	real
Ereignisse			
	Geschäftsvorfall		Klasse
	Leistungsprozess		Klasse
	IT-Ereignis		Klasse
Governance	IKS / IT-Management Lenkung		

*) Für die Verfahrensdokumentation werden die Namen der Mitarbeiter in diesem Kontext nicht benötigt, da im jeweiligen Journal eine Identifikation des MA direkt oder codiert erfolgt. Deshalb können die Daten zur Identifikation des konkreten MA auch in einem anderen System geführt werden. Sollte jedoch der konkrete MA im Rahmen des IKS als Risiko- bzw. Kontrollobjekt identifiziert werden, empfiehlt sich die Führung der Daten unter Organisation/Personen.

Bevor es an die Modellierung der Ebene der Governance geht, sei hier kurz ein Definition aus Wikipedia (http://de.wikipedia.org/wiki/Governance) wiedergegeben: „Unter *Corporate Governance* versteht man die Kontroll- und Steuerungsstruktur innerhalb … privatwirtschaftlicher Unternehmen. Governance bezieht sich ausschließlich auf Strukturen und ist von "Regierungsführung" als Prozess zu unterscheiden."

Demgemäß soll hier „Struktur von Lenkung und Kontrolle" oder im Kontext der Modellierung kurz „Lenkung und Kontrolle" verwendet werden. Die Struktur soll wiederum durch Dokumentations-Objekte und deren Beziehungen zu anderen repräsentiert werden.

Zerlegung der Governance: Die wichtigsten im Sinne der GoBS wahrnehmbaren Bausteine der Governance sind das das Interne Kontrollsystem IKS und das IT-Management. Das IT-Management schafft durch das Enabling die Voraussetzungen dafür, dass überhaupt Geschäftsvorfälle elektronisch abgewickelt werden können, und wird deshalb als Instrument der Lenkungsstruktur mit einem eigenständigen Abschnitt eingeordnet.
Akzeptieren wir diese Sonderstellung und fassen unter Lenkung alle verbleibenden Elemente wie Policies, Risikobehandlung und („installierte") Standards zusammen, fehlt nur noch ein übergeordneter Punkt zur Identifikation der wichtigsten Unternehmensdaten.

IKS: Beim Durchforsten der Realität nach wahrnehmbaren Objekten, in denen sich Funktion und Struktur der Governance manifestieren, wird sich ein Dokumentationsmodell für das IKS nicht ohne normatives Vorurteil fassen lassen wie der Vergleich unterschiedlicher Ansätze in A Comparison of Internal Controls: COBIT®, SAC, COSO and SAS 55/78 zeigt. Diese lassen sich aber mit Hilfe eines Dokumentationsmodells darstellen, in dem die jeweiligen Klassifikatoren passend ersetzt werden. Auch der grundsätzliche Funktionszyklus ist anpassbar. Am Beispiel eines ideellen IKS soll das nachfolgend exerziert werden.

Dokumentationsmodell des IKS

Definition (eines) IKS: Das Interne Kontrollsystem (IKS) ist das Management-Werkzeug der unternehmensinternen betriebswirtschaftlichen Überwachung. Dieses Werkzeug wird in Form einer Fragestellung auf **Kontroll-Objekte** des Unternehmens angewandt; bei der Anwendung werden Kontroll-Ziele der **Zielfelder des IKS** verfolgt und als Ergebnis **IKS-Instrumente** geliefert. Das IKS wird auf das Unternehmen angewandt und selbst zu einem Kontroll-Objekt erklärt.

Instrumente: IKS-Instrumente werden einer der folgenden Klassen zugeordnet**:**

D1 Grundsätze	Policies, Richtlinien; Vorkehrung
D2 Organisation	Aufbau: Organisationsplan/Vorkehrung
D3 Einrichtungen	Techn. Installat., Kontr. /Vorkehrung
D4 Verfahren	Prozesse – Anweisungen - Kontrollen
D5 Maßnahmen	Management- Gestaltungseingriff

IKS-Instrumente sind das Ergebnis von IKS-Projekten. Erst nach ihrer Installation bzw. Implementierung werden Instrumente als IKS-Anwendungen in Form von Kontrollen, Vorkehrungen, Berichten etc. laufend angewandt. Das Instrument ist die Definition bzw. Dokumentation der Anwendung. Im einfachsten Fall kann dies eine Anweisung, ein Grundsatz etc sein. Dieser existiert in geschriebener Form, bedarf aber der Anwendung und Kontrolle auf Einhaltung (Anwendung).

Komponenten: Die als Komponenten nach IDW, COSO etc. (hier Operationsfelder) des IKS werden bezeichnet:

K1 Kontrollumfeld	Problembewusstsein, Unternehmenskultur
K2 Risikoerkennung	Erkennung & Analyse von Unternehmensrisiken
K3 Kontrollaktivitäten	Kontrollen (integriert, intellektuell), IKS-Kalender
K4 Information/ Kommunikation	Richtlinien, Handbücher, Berichte, Kontakte
K5 Überwachung des IKS	Beurteilung der Wirksamkeit des IKS

Zielfelder: Das IKS wird auf IKS-Objekte angewandt werden zur Erzielung von:

T1 Rechtskonformität	Einhaltung der rechtlichen Vorschriften (Compliance)
T2 Strategie-Adhärenz	Einhaltung der definierten Geschäftsstrategie
T3 Bilanz-Qualität	Ordnungsmäßigkeit der Rechnungslegung
T4 Prozess-Qualität	Sicherheit, Effizienz, Wirksamkeit betrieblicher Prozesse
T5 Asset-Schutz	Schutz von Gütern, Vermögen, Daten und Informationen

Ende der Definition (eines) IKS.

Das Klassifikator-Tripel DKT (Instrument, Komponente, Zielfeld/Target) wird nachfolgend zur Identifikation von Attributen genutzt.

Funktionaler Ablauf: Da es in den verschiedenen IKS-Modellen zu unterschiedlichen funktionalen Abläufen kommen kann, werden nur solche Objekte verwendet, die sich in einem Modell als Dokumentations-Objekte manifestieren. Der Ablauf wird durch die Anordnung dieser D-Objekte repräsentiert.

Bericht: Eine IKS-Aktivität wird durch einen „Bericht" ausgelöst: Bericht -> Aktivität. Der Bericht ist „regulär" oder „ad-hoc". Die regulären Berichte sind etablierte Informationsinstrumente (Monatsberichte, Abstimmlisten, Auswertungen des Berichtswesens etc.) und werden regelmäßig inspiziert bzw. nach Terminplanung. Der ad-hoc Bericht lieferte eine Information über ein potentielles IKS-Problem und bezieht sich auf ein Kontroll-Objekt, das in der obigen Tabelle „Dokumentations-Objekte" enthalten ist. Die Aktivität besteht in der Anwendung eines Bausteins auf das Kontroll-Objekt.

Baustein: Das auf ein konkretes Kontroll-Objekt anzuwendende Werkzeug heißt Baustein[1]. Der Baustein stellt einen Satz von Fragestellungen dar. Der Typ des Bausteins wird durch den Typ des Kontrollobjekts bestimmt. Das heißt, dass auf ein gewähltes Kontrollobjekte nur Fragestellungen eines bestimmten Typs anwendbar sind.
Baustein(j):= {Fragestellung(i)}; (i=1…j)
Anmerkung: Jede Fragestellung verfolgt ein Kontrollziel aus einem Zielfeld t ∈ {T1..T5}. Das Ergebnis der Untersuchung ist eine Instrumentmenge; jedes Instrument lässt sich einer Kategorie zuordnen. R_j=> {D1 .. D5}

IKS-Projekt: Diese Fragestellungen werden auf ein Kontroll-Objekt KOB angewandt und liefern ein Instrument bzw. eine Instrumentenmenge:
Baustein => KOB => {Instrument(D_i)}; (i ∈ 1..5)
Im Rahmen eines IKS-Projekts erfolgt die Ermittlung der Ergebnis-Instrumente, deren Implementierung als IKS-Anwendung und eventuell deren weitere Überwachung. Mit dem Eintritt in die reguläre Überwachung ist das IKS-Projekt abgeschlossen.
Eine besondere Position nimmt die universelle Fragestellung **Risiko** ein, die ein eigenes Operationsfeld (Komponente K2) des IKS darstellt und in jedem Baustein enthalten ist.
Das Ergebnis des IKS-Projekts besteht in einer Auswahlmenge von Instrumenten.
Die Instrumente werden implementiert und führen zu einer IKS-Anwendung.

IKS-Kalender: IKS-Ereignisse und geplante Kontrollhandlungen werden im IKS-Kalender eingetragen. Der Erhalt eines nicht-regulären Berichts wird zu den IKS-Ereignissen gerechnet. Für prozessintegrierte Kontrollen, deren Durchführung und Ergebnis automatisch erfasst werden können, empfiehlt sich die Führung eines IKS-Journals. Der Kalender sollte so gestaltet sein, dass einzelne Einträge mit den evtl. zugehörigen Dokumenten verkettet werden bzw. Hinweise/Links auf solche möglich sind. Der Kalender dient dem Nachweis von IKS-Ereignissen und der Planung von Kontrollaktivitäten.

Anmerkung: Als Anwendungen des IKS werden implementierte Instrumente bezeichnet wie Vorkehrungen und Kontrollen, und alle Elemente aus K2 – K5, der IKS-Kalender und die Aktionen der Beauftragung. Im IKS-Kalender werden Anwendungen, Berichte, Projekte und Termine für Kontroll-Aktivitäten eingetragen.

Ende des Dokumentationsmodells IKS
Fassen wir die D-Objekte des IKS noch einmal zusammen:

- IKS-Berichte (KT)
- IKS-Bausteine (KT)[2]
- IKS-Projekte (DKT)
- IKS-Anwendungen (DKT)
- IKS-Kalender (DKT)

so ergibt sich die Attribut-Gestalt der D-Objekte mit der Auswahl des jeweiligen IKS-Modells, aus den oben gelisteten D-Objekten und der Definition der inneren Gestalt des D-Objekts. Mehr oder weniger systematische Bausteinsammlungen finden sich ansatzweise auf den Seiten der ISACE und in zahlreichen Coso/Cobit-Veröffentlichungen.

---

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

[2] **Anmerkung:** Derartige Bausteinsammlungen gibt es nur wenig in systematischer Form. Doch helfen hier die zahlreichen Checklisten (IDW / DRS u.a.m.) ganz gut, wenn auch die möglichen Antworten fehlen.

Im Dokumentationsmodell des IKS fehlt noch ein wesentliches Element, das zum Verständnis von etablierten Strukturen, Einrichtungen, Grundsätzen beiträgt: IKS-Hinweise. Unter dieser Rubrik lassen sich Erläuterungen und Begründungen unterbringen, die einem Dritten ein schnelleres Verständnis IKS-relevanter Themen erlauben.

Risiko-Management

Für die Dokumentation des Risikomanagements wird ebenfalls ein Modell zur Darstellung eines Risiko-Objektes mit den entsprechenden Attributen benötigt. Dieses soll der Kommunikation und dem Nachweis der Durchführung von Risikoanalysen und darauf folgenden Entscheidungen dienen und ein „Deckblatt" für die Risiko-Untersuchung liefern.
Der Einfachheit halber wird hier das Modell der FERMA benutzt, der Federation of European Risk Management Professionals. Wichtig ist es, an dieser stelle noch mal darauf hinzuweisen, dass in diesem Dokumentationsmodell nur Ereignisse und Feststellungen dokumentiert werden, nicht die eigentlichen Arbeiten der Analyse etc.

Dokumentations-Objekt für RISIKO

Risikoidentifikation

Name	Depot WCC
Risikofeld	Wechselkurse
Risikoklasse	finanziell-extern
Risiko-Owner(Person)	
IT-Risiko-Objekt	

Risikobeschreibung

Tragweite	bis zu 30% Verlust möglich
Quantifizierung	250 Mio, p=70%
Risikotoleranz/Appetit	
Kontrollinstrumente	kurse, insider infos
Risikominderung	sofort verkaufen

Risikobeurteilung

Gefahren und Möglichkeiten - Finanz. Auswirkungen

Einschätztung-GM	hoch > €
Wert	

Gefahr/Chance - Eintrittswahrscheinlichkeit/-horizont

Gefahr/Chance	Gefahr
Wahrscheinlichkeit	sehr hoch >75%
Eintrittshorizont	3 M

Risikoanalyse - Methoden

Analyse-Methodik	Fuzzy-Anaylse und MonteCarlo-Progrnose kombiniert mit Social Agents Modell

Risikoprofil

Risiko-Owner(Abtlg.)	Firma
Projektstart	
Projekt-Horizont	
Projekt-Ende	
R-Bedeutsamkeit	sehr hoch
Prim. R-Priorisierungstool	
Prim. R-Kontrollinstrument	
Investition R-Kontrolle	erhöhen

Risikobewertung

Keine internen Risiken. Maximale Ordnungsstrafe 400 € per Annum.

Tabelle: Kriterien aus Abteilungen

Abteilung	Stellungnahme
Keine Einträge vorhanden	

Mögliche Kosten
Mögliche Leistungen
Rechtliche Auflagen
sozio-ökonom. Faktoren
weitere Einflußfaktoren

Risikobehandlung

Kontrolle	
Eindämmung	Pressearbeit, selbst hinzukaufen
Vermeidung	
Transfer	übertragen an Tochter X
Finanzierung	nicht versicherbar

Kostenrentabilität der Durchführung

Durchführungskosten der Kontrollmaßnahme bezogen (/) auf Risikosenkungsnutzen
Rentabilität
Unterlassungsverlust
Entscheidung für Kontrolle ja

Risikoberichterstattung

Vorstand	ja
Stakeholder	ja
Management	ja
Andere	

Die Klassifikatoren für die Attribute der einzelnen Abteilungen finden sich auf der Webseite der FERMA.

IT-Management: In welchen Objekten manifestiert sich das IT-Management? Am Anfang des Handelns stehen die Richtlinien. In schärferer Form als Vorgabe für die Abwicklung von IT-Handlungen im Felde treten Handlungsvorschriften auf, die hier als IT-Anweisungen[1] bezeichnet werden sollen. Diese betreffen das IT-Personal.
Solche Richtlinien, die das planerische und strategische IT-Vorgehen betreffen, sollen zu den die IT betreffenden IKS-Instrumenten gerechnet werden. Solche IT-Richtlinien, die alle Mitarbeiter betreffen, die per IT buchungspflichtige Geschäftsvorfälle abwickeln, sollen untern Anweisungen GVF (Geschäftsvorfälle) geführt werden.
IT-Anweisungen: IT-Management → IT-Personal
IT-Grundsätze: Leitung/Management/IKS → IT-Management
GVF-Anweisungen : Leitung/Management/IKS → Personal
Damit ist die IT-Anweisung auf eine Handlungsvorschrift für das IT-Personal als Muster für die Abwicklung von IT-Ereignissen eingeschränkt.
Unabhängig von den zahlreichen Tools, die eventuell zum Einsatz kommen, ist es für die Dokumentation relevant, dass ein IT-Ereignis stattgefunden hat. Als einfachstes und unverselles Mittel der Dokumentation bietet sich hier der Kalender. Es kann durchaus wünschenswert sein, die Aufzeichnungen über IT-Ereignisse aus den Prozessfeldern (z.B. Coso/Cobit): a) Planung & Organisation, b) Beschaffung & Installation, c) Betrieb und Service, d) Überwachung getrennt zu führen. Die strategischen und planerischen in einem IT-Kalender und die Operationen „im Feld" aus b) und c) in einem IT-Journal, ähnlich den Journalen bei der Aufzeichnung von Geschäftsvorfällen.
Ein Eintrag im IT-Journal wird wieder als Dokumentations-Objekt aufgebaut: Mitarbeiter, Datum/Zeit, betroffene IT-Komponenten, Typ des IT-Ereignisses (mit zugehörigem Prozess etc), Protokolle, Testate etc. und eine Kurzbeschreibung oder Typisierung des Ablaufs (normal, nicht durchführbar weil…, besondere Umstände:….). Ein entsprechendes D-Objekt lässt sich für den IT-Kalender nun leicht formulieren.
Doch hier fehlt noch ein Element, das einer eigenen Dokumentationsform bedarf: IT-Sicherheit. Mit den IT-Grundschutz nach dem GSHB des BSI ist die Form der Dokumentation vorgegeben; diese lässt sich ohne weiteres mit dem Hilfsmittel Dokumentations-Objekt abbilden.

Damit bleiben für das IT-Management vier Dokumentationsinstrumente übrig:

- IT-Richtlinien (inkl. Anweisungen)
- IT-Journal (Eintragung der durchgeführten IT-Ereignisse/Tasks durch MA)
- IT-Kalender (Planung und Durchführung von Nicht-Feld-Aktivitäten)
- IT-Sicherheit (etwa GSHB: Objekte/Gefährdungen/Maßnahmen)

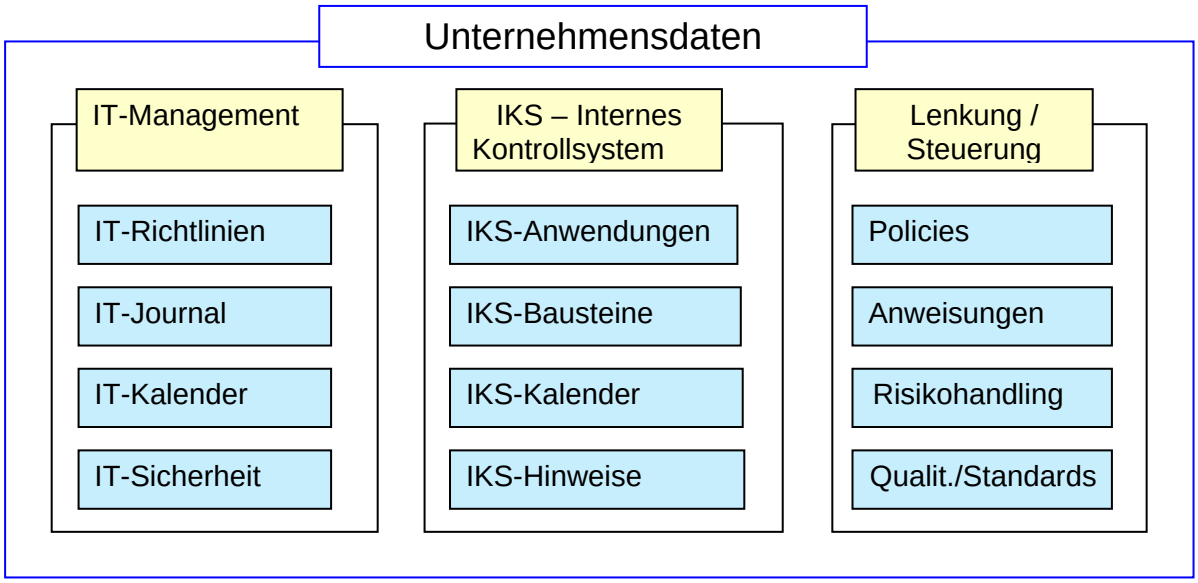
Lenkung/Steuerung: Auch auf der höchsten Ebene der Unternehmensgestaltung lassen sich Manifestations-Objekte identifizieren, die dem Verständnis des Verfahrens dienen. Ähnlich wie beim IT-Management finden wir zunächst Geschäftsgrundsätze, unternehmensweite Richtlinien und Anweisungen, Aufzeichnungen über den Umgang mit Risiken, das erreichte Niveau betreffend Standards (Qualität / Compliance / Rechnungslegung usw.). Mit dem Vorliegen eines Zertifikats bzgl. eines Standards werden einem Dritten grundsätzliche, für das Verfahren relevante Eigenschaften glaubhaft verdeutlicht. Aufgrund dieses Aufbaus gestalten sich die Dokumentations-Objekte entsprechend einfach. Das sind im Wesentlichen Tabellen, das Risikomanagement wie oben skizziert und Aussagen zu Standards bzw. Zertifikate.

Unternehmensdaten: Diese Objekte bedürfen keiner Erläuterung: Allgemeine Angaben, Bilanz, GuV, Lagebericht, Beteiligungen etc. Mit weiteren Angaben zur Organisation in Form von Organigrammen sind die verfahrensrelevanten Objekte hier ausgeschöpft.

Den Aufbau einer Dokumentationsstruktur für die Governance zeigt die nachfolgende Grafik. Damit sind der vorliegende Aufsatz und die vorhergehenden abgeschlossen.

---

[1] (Nach Wikipedia: Unter einer **Anweisung** versteht man eine (verbindliche) mündliche, gestikuläre, schriftliche oder digitale Äußerung, wie sich eine Person verhalten oder ein Vorgang ablaufen soll.



Schlussbemerkung

Abschließend sei noch einmal darauf hingewiesen, dass es sich in der vorliegenden Aufsatzreihe bei allen „Modellen" um „Dokumentationsmodelle" (für die GoBS oder SOX) handelt. Ziel aller „Modellchen" und Modelle ist einerseits die Nachbildung der Realität, d.h. von Objekten, die sich in der Realität manifestieren, aber andererseits auch die ständige Änderung der Realität mitzuschreiben.

Der Sinn der Modelle besteht natürlich darin, eine unmittelbare Beziehung zur bekannten Objekten (Server, Anwendung, Abteilung…..) herzustellen, und an diesen Objekten per Attribut das aufzuhängen, was die Verfahrensdokumentation nach GoBS verlangt.
Die GoBS selbst könnten strukturell wie dieses Modell aufgebaut wird, da sich alle aus den GoBS ableitbaren Forderungen per Attributbildung an der „richtigen Stelle" einklinken lassen. Sogar bei der Gestaltung des Textes ließe sich die Vererbung von Forderungen bzw. Eigenschaften gut ausnützen. Als Nebeneffekt käme es zu einer Standardisierung der Dokumentationsstruktur; damit könnte der Fiskus seinem Staatsauftrag „Prüfung" viel leichter nachkommen als bisher (was er ja kaum tut!). Aber offenbar ist das nicht beabsichtigt.

Dortmund, März 2007

Autorenhinweis
Siegfried Mack
www.aufbewahrungspflicht.de